eduSeal

Begleitdokument

Erläuterungen & Umsetzungshinweise

System-Anbieter in der Datenschutzrolle **Auftragsverarbeiter**

Stand 01.03.2026 | Version 1.0

eduSeal

Weitere Begleitdokumente

- Zertifizierungsgegenstand
- Risikobewertungskonzept
- Erläuterungen und Umsetzungshinweise
- Erläuterungen zum Zertifizierungsverfahren für System-Anbieter

Beitrag zum Forschungsprojekt „Data Protection Certification for Educational Information Systems (directions)“, das durch das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend gefördert wird (FKZ 01PP21003).

Projekt Webseite
www.directions-cert.de

Das Forschungsprojekt directions basiert auf den Ergebnissen und Dokumenten von AUDITOR (www.trusted-cloud.de).

Gefördert vom:

directions

Bundesministerium
für Bildung, Familie, Senioren,
Frauen und Jugend

Autoren

Jan Torben Helmke[a], Gerrit Hornung[a], Marcel Kohpeiß[a], Hendrik Link[a], Hans-Hermann Schild[a], Stephan Schindler[a], Kathrin Brecker[b], Philipp Danylak[c], Sebastian Lins[d], Eva Späthe[d], Ali Sunyaev[c]

[a] Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

[b] Forschungsgruppe Critical Information Infrastructures am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

[c] Chair of Information Infrastructures an der School of Computation am Campus Heilbronn der Technischen Universität München

[d] Fachgebiet Wirtschaftsinformatik, insb. Enterprise Systems and Platforms der Universität Kassel

Empfohlene Zitation
Helmke, Hornung, Kohpeiß, Link, Schild, Schindler, Brecker, Danylak, Lins, Späthe, Sunyaev (2026). eduSeal-Kriterienkatalog – Version 1.0. Online verfügbar: www.directions-cert.de.

Inhaltsverzeichnis

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen in diesem Dokument sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, so dass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z. B. ist bei der Bezeichnung *System-Anbieter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interfaces
Art.	Artikel
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (letzte berücksichtigte Änderung: 25.07.2025)
BaySchO	Bayerische Schulordnung (letzte berücksichtigte Änderung: 04.07.2025)
BBG	Bundesbeamtengesetz (letzte berücksichtigte Änderung: 27.02.2025)
BbgSchulG	Brandenburgisches Schulgesetz (letzte berücksichtigte Änderung: 23.06.2025)
BDSG	Bundesdatenschutzgesetz (letzte berücksichtigte Änderung: 06.05.2024)
BeamtStG	Beamtenstatusgesetz (letzte berücksichtigte Änderung: 20.12.2023)
BORA	Berufsordnung für Rechtsanwälte (letzte berücksichtigte Änderung: 26.05.2025)
BRAO	Bundesrechtsanwaltsordnung (letzte berücksichtigte Änderung: 22.12.2025)
BremSchulDSG	Bremisches Schuldatenschutzgesetz (letzte berücksichtigte Änderung: 01.04.2025)
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
COBIT	Control Objectives for Information and Related Technology
Cross-VM Attacks	Angriffe über virtuelle Maschinen
CVSS	Common Vulnerability Scoring System
d.h.	das heißt
DigLLV Berlin	Verordnung über die Verarbeitung personenbezogener Daten beim Einsatz von digitalen Lehr- und Lernmitteln und sonstigen pädagogischen Zwecken dienenden digitalen Instrumenten (Berlin) (letzte berücksichtigte Änderung: 04.03.2024)
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung (letzte berücksichtigte Änderung: 04.03.2021)
DSK	Datenschutzkonferenz
DSV-BBG	Datenschutzverordnung Schulwesen des Landes Brandenburg (letzte berücksichtigte Änderung: 02.09.2020)
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss
EG	Erwägungsgrund
EGMR	Europäischer Gerichtshof für Menschenrechte
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-SVK	EU-Standardvertragsklauseln
EWR	Europäischer Wirtschaftsraum
f.	folgend
ff.	folgende
FISA	Foreign Intelligence Sourveillance Act
GDPR	General Data Protection Regulation (letzte berücksichtigte Änderung: siehe DS-GVO)
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
ggf.	gegebenenfalls
GPA	Global Privacy Assembly
GRCh	Charta der Grundrechte der Europäischen Union (letzte berücksichtigte Änderung: 12.12.2007)
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit

HmbSG	Hamburgisches Schulgesetz (letzte berücksichtigte Änderung: 27.05.2024)
Hs.	Halbsatz
i.d.R.	In der Regel
i.d.S.	In diesem Sinne
i.S.d.	Im Sinne des
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
ID	Identifier
IDM	Identitätsmanagement
IKEv2	Internet Key Exchange
IPSec	Internet Protocol Security
ISO	Internationale Organisation für Normung
ITIL	Information Technology Infrastructure Library
JSON-Format	JavaScript Object Notation
LDSG	Landesdatenschutzgesetz
LDSG-BW	Landesdatenschutzgesetz Baden-Württemberg (letzte berücksichtigte Änderung: 29.07.2025)
LfD	Landesbeauftragte für Datenschutz
lit.	Litera
NGO	Non-governmental organization
Nr.	Nummer
NSchulG	Niedersächsisches Schulgesetz (letzte berücksichtigte Änderung: 25.06.2025)
OSS	Open-Source-Software
PETS	Privacy Enhancing Technologies
RdErl.	Runderlass
RL	Richtlinie
s.	siehe
S.	Satz
s.a.	siehe auch
s.o.	siehe oben
SächsSchulG	Sächsisches Schulgesetz (letzte berücksichtigte Änderung: 17.07.2024)
SchDSV-HE	Verordnung über die Verarbeitung personenbezogener Daten durch Schulen und Schulaufsichtsbehörden (Hessen) (letzte berücksichtigte Änderung: 16.12.2023)
SchDVVO Bremen	Verordnung über die Datenverarbeitung durch Schulen und Schulbehörden (Bremen) (letzte berücksichtigte Änderung: 17.11.2011)
SchoG SL	Schulordnungsgesetz (Saarland) (letzte berücksichtigte Änderung: 25.06.2025)
SchulDatenV Berlin	Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Berlin) (letzte berücksichtigte Änderung: 04.03.2024)
SchulDSV HA	Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Hamburg) (letzte berücksichtigte Änderung: 23.09.2025)
SchulDSVO M-V	Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal des Landes Mecklenburg-Vorpommern (letzte berücksichtigte Änderung: 24.04.2020)
SchulDSVO SH	Landesverordnung über die Verarbeitung personenbezogener Daten an öffentlichen Schulen des Landes Schleswig-Holstein (letzte berücksichtigte Änderung: 27.09.2024)
SchulG BW	Schulgesetz Baden-Württemberg (letzte berücksichtigte Änderung: 29.01.2025)
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt (letzte berücksichtigte Änderung: 05.06.2025)
SchulG M-V	Schulgesetz für das Land Mecklenburg-Vorpommern (letzte berücksichtigte Änderung: 24.03.2025)
SchulG NRW	Schulgesetz für das Land Nordrhein-Westfalen (letzte berücksichtigte Änderung: 27.05.2025)
SchulG SH	Schleswig-Holsteinisches Schulgesetz (letzte berücksichtigte Änderung: 29.01.2025)
SchulG-BE	Schulgesetz Berlin (letzte berücksichtigte Änderung: 10.07.2024)

SchulG-HE	Hessisches Schulgesetz (letzte berücksichtigte Änderung: 30.06.2025)
SchulG-RLP	Schulgesetz Rheinland-Pfalz (letzte berücksichtigte Änderung: 20.12.2024)
SchulStat-DVV BW	Verordnung des Kultusministeriums über die Datenverarbeitung für statistische Erhebungen und schulübergreifende Verwaltungszwecke an Schulen für das Land Baden-Württemberg (letzte berücksichtigte Änderung: 10.07.2008)
SchulO-RLP	Schulordnung Rheinland-Pfalz (letzte berücksichtigte Änderung: 01.01.2009)
SchulwDSG SL	Gesetz über den Schutz personenbezogener Daten im Schulwesen Saarland (Schulwesen-Datenschutzgesetz) (letzte berücksichtigte Änderung: 10.07.2024)
SchulwDSV SL	Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Schulwesen Saarland (Schulwesen-Datenschutzverordnung) (letzte berücksichtigte Änderung: 10.07.2024)
SDM	Standard-Datenschutzmodell
SSH	Secure Shell
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch (letzte berücksichtigte Änderung: 13.11.2024)
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (letzte berücksichtigte Änderung: 2.12.2025)
ThürASObbS	Thüringer Allgemeine Schulordnung für die berufsbildenden Schulen (letzte berücksichtigte Änderung: 24.05.2024)
ThürSchulG	Thüringer Schulgesetz (letzte berücksichtigte Änderung: 02.07.2024)
ThürSchulO	Thüringer Schulordnung (letzte berücksichtigte Änderung: 06.06.2024)
TLS	Transport Layer Security
TOM	technische und organisatorische Maßnahme
u.a.	unter anderem
UAbs.	Unterabsatz
Urt.	Urteil
USA	United States of America
VO-DV I NRW	Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen und Schülern und Eltern (Nordrhein-Westfalen) (letzte berücksichtigte Änderung: 01.08.2022)
VO-DV II NRW	Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer sowie des sonstigen Personals im Schulbereich (Nordrhein-Westfalen) (letzte berücksichtigte Änderung: 21.12.2021)
VollzBek DS Bay	Vollzug des Datenschutzrechts an staatlichen Schulen (Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus vom 14. Juli 2022)
VwV	Verwaltungsvorschrift
VwV Schuldatenschutz Sachsen	Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über den Datenschutz bei der Verarbeitung personenbezogener Daten an Schulen (letzte berücksichtigte Änderung: 11.07.2018)
VwV Schulformulare Sachsen	Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus zur Verwendung von Formularen für die schulische Verwaltung an allgemeinbildenden Schulen und Schulen des zweiten Bildungsweges (letzte berücksichtigte Änderung: 01.12.2023)
VwV-Datenschutz an öffentlichen Schulen BW	Verwaltungsvorschrift des Kultusministeriums über den Datenschutz an öffentlichen Schulen (Baden-Württemberg) (letzte berücksichtigte Änderung: 04.07.2019)
XML-Format	Extensible Markup Language
z. B.	zum Beispiel
Ziff.	Ziffer

A. Kriterien für System-Anbieter als Auftragsverarbeiter

Kapitel I: Rechtsverbindliche Vereinbarung über die Auftragsverarbeitung

Erläuterung

Bei der Zertifizierung von Auftragsverarbeitern (hier: System-Anbieter) müssen diese nachweisen, dass sie (und ihre ggf. eingebundenen Unterauftragsverarbeiter) die in ihrem Machtbereich liegenden erforderlichen TOM getroffen haben. Die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter darf gemäß Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO nur auf Grundlage eines Vertrages (in den Kriterien als „rechtsverbindliche Vereinbarung über die Auftragsverarbeitung" bezeichnet) erfolgen.[1] Ohne einen entsprechenden Vertrag darf der Auftragsverarbeiter keine personenbezogenen Daten für den Verantwortlichen verarbeiten. Die gesetzlichen Anforderungen an den Vertrag werden durch die nachfolgenden Kriterien in Nr. 1 konkretisiert.

In der Praxis kann das Problem auftreten, dass die für Schulen (System-Kunden) zuständigen staatlichen Stellen Auftragsverarbeitungsverträge vorgeben, denen der Auftragsverarbeiter (System-Anbieter) letztlich zustimmen muss. Die staatlichen Stellen sollten daher die Anforderungen dieses Kriterienkatalogs bei Gestaltung der Auftragsverarbeitungsverträge beachten, da die Zertifizierung andernfalls unwirksam sein kann, wenn die vorgegebenen Auftragsverarbeitungsverträge nicht den Anforderungen dieses Kriterienkatalogs entsprechen. Im Grundsatz sollten Konflikte aber nicht auftreten oder beherrschbar sein, da auch die von staatlichen Stellen verwendeten Auftragsverarbeitungsverträge die im Kriterienkatalog konkretisierten Anforderungen der DS-GVO einhalten müssen.

Nr. 1 – Rechtsverbindliche Vereinbarung über die Auftragsverarbeitung zwischen System-Anbieter und System-Kunde
(Art. 28 Abs. 3 DS-GVO)

Nr. 1.1 – Verarbeitung aufgrund einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung und Form der Vereinbarung
(Art. 28 Abs. 3 UAbs. 1 Satz 1 und Abs. 9 DS-GVO)

Kriterium

1) Der System-Anbieter stellt sicher, dass er eine rechtsverbindliche Vereinbarung über die Auftragsverarbeitung mit dem System-Kunden abschließt.

2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

3) Diese rechtsverbindliche Vereinbarung über die Auftragsverarbeitung muss die Kriterien dieses Kapitels erfüllen, wobei die in diesen Kriterien geforderten Festlegungen nicht zwingend in einem einzigen, sondern auch in verschiedenen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung einbezogen worden sind.

Erläuterung

Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung ist wesentlich, da mit dieser die Rolle des System-Anbieters als Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DS-GVO gegenüber der

[1] Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO schreibt die Auftragsverarbeitung auf Grundlage eines Vertrags vor. Alternativ zum Vertrag kann auch ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten im Sinne des Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO als Rechtsgrundlage für die Auftragsverarbeitung dienen.

Rolle des System-Kunden als Verantwortlichem ausdrücklich klargestellt wird. Ohne eine rechtsverbindliche Vereinbarung darf der System-Anbieter keine personenbezogenen Daten für den System-Kunden verarbeiten.

Oft liegt dieser rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung eine weitere Vereinbarung über die Leistungserbringung zugrunde. Beide Vereinbarungen sind zu unterscheiden. Die Vereinbarung ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 9 DS-GVO). Dieses Formerfordernis verlangt keine qualifizierte Signatur i.S.v. § 126a BGB. Es genügt auch Textform i.S.v. § 126b BGB.

Umsetzungshinweis

Um sicherzustellen, dass eine Vereinbarung geschlossen wurde, kann der System-Anbieter TOM vorsehen, z. B. Freischaltung des schulischen Informationssystems für den System-Kunden erst nach Vorlage der unterschriebenen Vereinbarung. Denkbar sind auch Vermittlerlösungen, bei denen der System-Anbieter sein schulisches Informationssystem z. B. über einen Vermittlungsdienst anbietet, der dann als Vertreter oder Bote des System-Anbieters dafür sorgt, dass die Vereinbarung zwischen dem System-Anbieter und dem System-Kunden zustande kommt.

Im Falle eines elektronischen Vertragsabschlusses (bzw. einer elektronischen Registrierung) kann dies dadurch sichergestellt werden, dass dem potenziellen System-Kunden eine entsprechende Vereinbarung angezeigt wird, die dieser vor der Systemnutzung bestätigt. Werden vorformulierte Vertragsklauseln (AGB) eingesetzt, müssen diese wirksam im Sinne des jeweiligen AGB-Rechts sein.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- ISO/IEC 27701:2025 Ziff. B.2.2.2 Kundenvereinbarung

Nr. 1.2 – Gegenstand und Dauer der Verarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO)

Kriterium

1) Der Gegenstand und die Dauer der Verarbeitung sind in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festzulegen.

2) Die Dauer der Verarbeitung kann in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung durch Angabe eines Start- oder Endpunktes, den Verweis auf eine unbestimmte Nutzungszeit oder andere geeignete Angaben erfolgen.

Umsetzungshinweis

Für den System-Anbieter und den System-Kunden sollte anhand dieser Eingrenzung des Auftragsgegenstands aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung klar hervorgehen, welche Verarbeitungsvorgänge (z. B. bzgl. der Verarbeitung der Daten von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten) durch den System-Anbieter für den System-Kunden durchgeführt werden. Insbesondere sollte in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung in transparenter Form dargelegt werden, welche Einflussmöglichkeiten dem System-Anbieter bei der Wahl der Verarbeitungsmittel zur Ausführung von Verarbeitungsvorgängen, in denen personenbezogene Daten verarbeitet werden, zukommen. Regelungen zum Auftragsgegenstand haben auch die abgegrenzten Verantwortungsbereiche zwischen System-Kunde und System-Anbieter abzubilden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Ziffer 7.3 Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- ISO/IEC 27701:2025 Ziff. B.2.2.2 Kundenvereinbarung

Nr. 1.3 – Art und Zweck der Datenverarbeitung, Art der verarbeiteten Daten, Kategorien betroffener Personen
(Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO)

Kriterium

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung werden Art und Zweck der vorgesehenen Verarbeitung von Daten im Auftrag, die Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt.

Umsetzungshinweis

Es ist zunächst zulässig, dass der System-Anbieter eine allgemeine Beschreibung von Art und Zweck der Datenverarbeitung, der Art der verarbeiteten Daten sowie den Kategorien betroffener Personen liefert. Allerdings sollten die Informationen in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung dann konkretisiert werden und auf die spezifische Verarbeitungssituation zugeschnitten sein, z. B. durch Angabe vordefinierter Datenarten, Kategorien betroffener Personen oder typischer Funktionen zur Erreichung bestimmter Datenverarbeitungszwecke. Die Beschreibung sollte möglichst präzise und konkret sein.

Allgemeine Angaben zu Art und Zweck der Datenverarbeitung wie z. B. „legitime Zwecke aller Art", „Betrieb von Bildungssoftware" oder „Bereitstellung digitaler Unterrichtsinhalte" sind nicht ausreichend. Die einzelnen Verarbeitungsschritte (z. B. Erheben, Speichern, Übermitteln) sind zu klären und „möglichst eindeutig und vollständig" festzulegen.[2] Z. B. sollte bei einem Identitätsmanagementsystem, an das weitere schulische Informationssysteme angebunden sind, die Datenweiterleitung zwischen den verschiedenen Systemen beschrieben werden. Erforderlich ist zudem eine Unterscheidung zwischen Daten von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten sowie ggf. weiteren betroffenen Personen. Die Daten, die zu diesen Datenkategorien gehören, sind näher zu bezeichnen. Werden – wie dies bei schulischen Informationssystemen regelmäßig der Fall sein wird – Daten Minderjähriger verarbeitet, sollte dies besonders berücksichtigt und dokumentiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 41 „Planen und Spezifizieren"
- SDM-Baustein 42 „Dokumentieren"
- ISO/IEC 27701:2025 Ziff. B.2.2.2 Kundenvereinbarung

Nr. 1.4 – Festlegung von Weisungsbefugnissen
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a, UAbs. 2 DS-GVO)

Kriterium

1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des System-Kunden – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation – verarbeitet werden, sofern der System-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist.

2) Für den Fall, dass der System-Anbieter durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist, sieht die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Pflicht des System-Anbieters vor, dem System-Kunden die

[2] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 53.

rechtlichen Anforderungen vor der Verarbeitung mitzuteilen, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3) Für den Fall, dass die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen auf Weisung des Verantwortlichen vorsieht, legt die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung fest, welche Instrumente nach Art. 45 DS-GVO oder Art. 46 Abs. 2 und 3 DS-GVO für die Übermittlungen genutzt und ggf. welche zusätzlichen Maßnahmen ergriffen werden sollen, um ein angemessenes Schutzniveau sicherzustellen.

4) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der System-Anbieter zur Information des System-Kunden, wenn er der Auffassung ist, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung gegen datenschutzrechtliche Vorschriften verstößt.

Erläuterung

Die Weisungsgebundenheit wird in der DS-GVO an mehreren Stellen genannt (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a, UAbs. 2 DS-GVO, indirekt in Art. 28 Abs. 10, Art. 29 und Art. 32 Abs. 4 DS-GVO) und stellt das Wesensmerkmal der Auftragsverarbeitung dar.

Weisungen sind zunächst die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung enthaltenen Festlegungen zu den Leistungen einschließlich TOM, die von dem Auftragsverarbeiter (hier dem System-Anbieter) zu erbringen sind. Weisungen können aber auch im laufenden Auftragsverhältnis erteilt werden.[3]

Überschreitet der System-Anbieter die Maßgaben des System-Kunden, so liegt ein Fall des Art. 28 Abs. 10 DS-GVO sowie ein Verstoß gegen Art. 29 DS-GVO vor, und der System-Anbieter hat mit haftungsrechtlichen Konsequenzen zu rechnen.

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a DS-GVO kann die Weisungsbefolgung den System-Anbieter jedoch nicht von der Gesetzestreue entbinden, so dass der System-Anbieter nicht-weisungsgedeckte Verarbeitungen durchführen darf, wenn er durch Unionsrecht oder mitgliedstaatliches Recht hierzu verpflichtet wird. Mit dieser Regelung soll Interessenkonflikten auf Seiten des System-Anbieters vorgebeugt werden.

Gemäß Art. 28 Abs. 3 UAbs. 2 DS-GVO hat der Auftragsverarbeiter (hier der System-Anbieter) den Verantwortlichen (hier den System-Kunden) unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt (s. hierzu Nr. 5.1). Diese Pflicht ist in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festzuhalten.

Umsetzungshinweis

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung des System-Anbieters sollten die Weisungsbefugnisse des System-Kunden aufgeführt werden. Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sollte die Rechte des System-Kunden zur Weisung des System-Anbieters beschreiben, inklusive der Rechte zur Änderung, Anpassung und Rücknahme von Weisungen. Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sollte nicht die Rechte des System-Kunden, Weisungen zu erteilen, beschränken, um die DS-GVO-konforme Verarbeitung gewährleisten zu können. System-Kunden können ihre Weisungen händisch oder mit automatisierten Verfahren und Funktionen (bspw. durch API-Aufrufe, Softwarebefehle oder Anklicken von Dienst-Funktionen; denkbar ist auch ein Ticketsystem) erteilen.

Aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sollte hervorgehen, ob weisungsgebundene Datenübermittlungen an Drittländer oder internationale Organisationen im Rahmen der Auftragsverarbeitung durchgeführt werden sollen und wie dort ein angemessenes Schutzniveau sichergestellt werden soll. Geeignete Garantien für die Datenübermittlung sind z. B. Standarddatenschutzklauseln der Kommission nach Art. 46 Abs. 2 lit. c DS-GVO oder ein genehmigtes Zertifizierungsverfahren nach Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DS-GVO. Darüber hinaus sollten zusätzliche Maßnahmen festgelegt werden, wenn ein angemessenes Schutzniveau nicht allein durch die Instrumente nach Art. 46 Abs. 2 und 3 DS-GVO erreicht werden kann (s. hierzu auch Nr. 14.1.). Das vorliegende eduSeal-Zertifizierungsverfahren selbst bietet keine Zertifizierung

[3] Taeger/Gabel/*Gabel/Lutz*, Art. 28 DS-GVO Rn. 42.

nach Art. 46 Abs. 2 lit. f DS-GVO. Der System-Anbieter darf beim System-Kunden nicht den Eindruck erwecken, dass es sich um eine Zertifizierung nach Art. 46 Abs. 2 lit. f DS-GVO handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Ziffer 7.1 Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- ISO/IEC 27701:2025 Ziff. B.2.2.3 Ziele der Organisation
- ISO/IEC 27701:2025 Ziff. B.2.2.5 Verstoßende Anweisungen

Nr. 1.5 – Ort der Datenverarbeitung
(Art. 28 Abs. 3 UAbs. 1 DS-GVO)

Kriterium

1) Aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung geht hervor, ob die Datenverarbeitung innerhalb der EU bzw. des EWR oder in einem Drittland stattfindet. Wird die Datenverarbeitung in einem Drittland durchgeführt, geht das Drittland aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung hervor.

2) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung wird festgelegt, dass der System-Anbieter den System-Kunden (also dessen befugte Mitarbeitende) unverzüglich informiert, wenn die Datenverarbeitung während des Geltungszeitraums der rechtsverbindlichen Vereinbarung aus der EU bzw. dem EWR in ein Drittland verlegt wird.

Erläuterung

Es muss aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung hervorgehen, ob die Datenverarbeitung an sich innerhalb der EU bzw. des EWR oder in einem Drittland stattfindet. Dies gilt auch für Verarbeitungstätigkeiten durch weitere Auftragsverarbeiter (sog. Subauftragsverarbeiter), wenn der System-Anbieter einen anderen Auftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Verantwortlichen beauftragt.

Wenn das schulspezifische Landesrecht, dem der System-Kunde unterliegt, eine Verarbeitung personenbezogener Daten außerhalb des EU- oder EWR-Raums verbieten sollte, hat der System-Anbieter durch TOM sicherzustellen, dass eine solche Verarbeitung nicht erfolgt. Etwa schließt in Baden-Württemberg Ziffer 1.14 VwV-Datenschutz an öffentlichen Schulen BW eine Verarbeitung aus, wenn diese an Serverstandorten in Drittländern, d.h. Ländern, die nicht dem EU/EWR Raum angehören (vgl. Art. 44 ff. DS-GVO), durchgeführt werden.

Nicht immer verhindert die ausschließliche Datenverarbeitung in der EU oder im EWR, dass personenbezogene Daten dem Zugriff staatlicher Stellen von Drittländern entzogen werden. So kann es Regelungen in den nationalen Gesetzen von Drittländern geben, die Auftragsverarbeiter im Drittland verpflichten, drittstaatlichen Stellen Zugriff auf in der EU oder im EWR verarbeitete personenbezogene Daten zu gewähren. Unterliegt ein System-Anbieter einer solchen Regelung, ist die Auswahl eines solchen Anbieters nicht grundsätzlich verboten, jedoch sollten System-Kunden und System-Anbieter (gemeinsam) Lösungen finden, um die personenbezogenen Daten effektiv vor dem Zugang der staatlichen Stellen des betreffenden Drittlands zu schützen. Für schulische Informationssysteme kann eine Verschlüsselung der Daten eine Lösung sein, um auf diese Weise zu verhindern, dass drittstaatliche Stellen Kenntnis vom Inhalt der Daten nehmen können. Eine weitere Möglichkeit ist z. B. die Einschaltung eines Treuhänders, der ausschließlich europäischem Recht unterliegt und der ausschließlich Zugriff auf die ausgelagerten Daten des System-Kunden hat. Durch die Treuhandvereinbarung sind die personenbezogenen Daten weder im Besitz noch unter der Kontrolle des System-Anbieters und könnten daher nicht an drittstaatliche Stellen herausgegeben werden.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2025 Ziff. B.2.5.2 Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen
- ISO/IEC 27701:2025 Ziff. B.2.5.3 Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können

Nr. 1.6 – Verpflichtung zur Vertraulichkeit
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b DS-GVO)

Kriterium

Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen des System-Anbieters vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

Erläuterung

Die Verpflichtung von Beschäftigten zur Vertraulichkeit ist ein wichtiger Bestandteil der Maßnahmen, die erforderlich sind, damit ein Auftragsverarbeiter die Einhaltung der Grundsätze der DS-GVO sicherstellen und nachweisen kann.[4] Hierdurch wird das Gewährleistungsziel der Vertraulichkeit (SDM C1.4) gefördert.

Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b DS-GVO verlangt, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (s. hierzu auch Nr. 6).

Von angemessenen gesetzliche Verschwiegenheitspflichten ist in Deutschland z. B. für Ärzte (§ 203 Abs. 1 Nr. 1 StGB), Beamte (§ 203 Abs. 2 Satz 1 Nr. 1 StGB, § 37 BeamtStG,[5] § 67 BBG), Rechtsanwälte (§ 43a Abs. 2 BRAO, § 2 BORA, § 203 Abs. 1 Nr. 3 StGB), staatlich anerkannte Sozialarbeiter sowie staatlich anerkannte Sozialpädagogen (§ 203 Abs. 1 Nr. 6 StGB) auszugehen.[6] Die DSK nennt beispielhaft Verschwiegenheitspflichten für privatärztliche, steuerberaterliche oder anwaltliche Verrechnungsstellen.[7] Für Beschäftigte im öffentlichen Dienst gilt § 203 Abs. 2 Satz 1 Nr. 2 StGB i.V.m. dem VerpflG. Bei einem typischen (privatrechtlichen) System-Anbieter werden diese gesetzlichen Verschwiegenheitspflichten indes regelmäßig nicht einschlägig sein.

Das GeschGehG begründet keine angemessene gesetzliche Verschwiegenheitspflicht i.d.S., da das Gesetz den Schutz personenbezogener Daten bzw. der Privatsphäre nicht adressiert.

Dass die Vertraulichkeitspflicht der zur Datenverarbeitung befugten Personen des System-Anbieters über das Ende ihres Beschäftigungsverhältnisses hinaus fort gilt, geht nicht explizit aus dem Wortlaut des Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b DS-GVO hervor. Nach dem Sinn und Zweck der Norm sollte diese Vertraulichkeitspflicht jedoch über das Ende des Beschäftigungsverhältnisses fortgelten, da ansonsten kein angemessener Schutz von personenbezogenen Daten gewährleistet werden kann.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO
- ISO/IEC 27002:2024 Ziff. 6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- ISO/IEC 27701:2025 Ziff. B.3.18 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

[4] DSK, Kurzpapier Nr. 19, S. 1.
[5] S.a. BeckOK Beamtenrecht Bund/*Weinrich*, § 37 BeamtenStG Rn. 24 bzgl. datenschutzrechtlicher Belange.
[6] Paal/Pauly/*Martini*, Art. 28 DS-GVO Rn. 43b.
[7] DSK, Kurzpapier Nr. 19, S. 1.

Nr. 1.7 – Datensicherheit und Unterstützung des System-Kunden durch den System-Anbieter bei Erfüllung der Pflichten nach Kapitel III und Art. 32 bis 36 DS-GVO

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c, e und f i.V.m. Kapitel III und Art. 32 bis 36 DS-GVO)

Kriterium

1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass der System-Anbieter alle gemäß Art. 32 DS-GVO erforderlichen TOM ergreift, um ein angemessenes Maß an Datensicherheit zu gewährleisten. Die TOM werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung beschrieben. Die Beschreibung enthält insbesondere die Angabe, ob der System-Anbieter eine Pseudonymisierung, Anonymisierung oder Verschlüsselung der zu verarbeitenden personenbezogenen Daten vornimmt.

2) Der System-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau er nach einem physischen oder technischen Zwischenfall die Daten sowie das schulische Informationssystem wiederherstellen und Zugang zum schulischen Informationssystem und zu den Daten sicherstellen kann.

3) Die Verfahren und Prozesse zur Unterstützung des System-Kunden bei der Erfüllung der Betroffenenrechte gemäß Kapitel III DS-GVO, bei der Einhaltung von Art. 32 DS-GVO, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 und 36 DS-GVO und bei Erfüllung der Meldepflichten bei Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DS-GVO werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

Umsetzungshinweis

Angaben zu den gemäß Art. 32 DS-GVO zu ergreifenden TOM zur Datensicherheit (Nr. 3) sollten möglichst konkret erfolgen.[8] Dies bedeutet indes nicht, dass jede einzelne TOM aufgezählt werden muss. Für den System-Kunden ist es wichtig zu wissen, welches Schutzniveau das schulische Informationssystem bietet. Die Angaben zur Pseudonymisierung (Nr. 3.9), Anonymisierung (Nr. 3.10) oder Verschlüsselung (Nr. 3.11) sollten klarstellen, ob diese Mechanismen auch gegenüber den Mitarbeitenden des System-Anbieters wirksam sind, die Zugang zu personenbezogenen Daten haben können.

Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung soll die Unterstützungspflichten des System-Anbieters gegenüber dem System-Kunden – dies betrifft die Unterstützung bei der Wahrnehmung der Pflichten nach Kapitel III DS-GVO (Betroffenenrechte, Nr. 7), Art. 32 DS-GVO (Datensicherheit, Nr. 9), Art. 33 und 34 DS-GVO (Meldepflichten, Nr. 2.2) sowie Art. 35 und 36 DS-GVO (Datenschutz-Folgenabschätzung, Nr. 10) – unter Berücksichtigung der Ausgestaltung des konkreten schulischen Informationssystems und der dem System-Anbieter zumutbaren und geeigneten TOM konkretisieren. Dies soll Unsicherheiten hinsichtlich der sich aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung ergebenden Rechte und Pflichten vermeiden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Ziffer 7.4 Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- EDSA, Guidelines 01/2025 on Pseudonymisation
- ISO/IEC 27701:2025 Ziff. B.2.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- ISO/IEC 27701:2025 Ziff. B.2.3 Verpflichtungen gegenüber betroffenen Personen

[8] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 68.

Nr. 1.8 – Inanspruchnahme der Dienste weiterer Auftragsverarbeiter (Subauftragsverarbeiter) durch den System-Anbieter
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. d DS-GVO)

Kriterium

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der System-Anbieter, die Bedingungen gemäß Art. 28 Abs. 2 und 4 DS-GVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einzuhalten.

Umsetzungshinweis

Die Anforderungen an die Inanspruchnahme weiterer Auftragsverarbeiter werden in den Kriterien in Nr. 13 präzisiert.

Soweit dem System-Kunden im Falle einer allgemeinen Genehmigung bei Änderungen in der Unterbeauftragung ein Einspruchsrecht zusteht (Nr. 13.1 Abs. 3), sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Voraussetzungen und Folgen eines Einspruchs geregelt werden. Dies betrifft insbesondere die Frage, ob die rechtsverbindliche Vereinbarung zur Auftragsvereinbarung bei Einspruch gekündigt werden darf.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- ISO/IEC 27701:2025 Ziff. B.2.5.7 Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden
- ISO/IEC 27701:2025 Ziff. B.2.5.8 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.2.5.9 Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten

Nr. 1.9 – Rückgabe und Löschung von Daten
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g DS-GVO)

Kriterium

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sind die Pflichten des System-Anbieters zur Rückgabe überlassener Datenträger, die personenbezogene Daten enthalten, sowie zur Rückgabe oder irreversiblen Löschung aller personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen festzulegen, sofern nicht nach nationalem Recht oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht.

Erläuterung

Datenträger i.d.S. sind Materialien, in oder auf denen Daten aufgezeichnet werden können und von denen Daten abgerufen werden können (ISO/IEC 2382:2015, Informationstechnik - Vokabular, Ziffer 2121321 „Datenträger“; s.a. Nr. 12).

Ist der System-Anbieter auch nach Ende der Auftragsverarbeitung aufgrund gesetzlicher Pflichten aus nationalem Recht oder Unionsrecht zur Speicherung oder Aufbewahrung von Daten verpflichtet, sind diese nicht zu löschen oder zurückzugeben. Eine rechtliche Verpflichtung hierzu, die aus einem Drittstaat herrührt, ist dafür nicht hinreichend.

Umsetzungshinweis

Der Nachweis der Rückgabe von Datenträgern und der Löschung von Daten sollte auch durch Verweis auf entsprechende Grundsätze des System-Anbieters erfolgen. Der System-Kunde sollte zwischen den Ausführungsmodalitäten wählen können.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2025 Ziff. B.2.4.3 Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten

Bezüglich der Aufbewahrungspflichten in der Schule s.a. Nr. 5.5.

Nr. 1.10 – Überprüfung des System-Anbieters durch den System-Kunden
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO)

Kriterium

1) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung ist die Verpflichtung des System-Anbieters festzulegen, alle Informationen zur Verfügung zu stellen, die für den Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten notwendig sind.

2) Ebenso ist in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festzulegen, dass der System-Anbieter Überprüfungen, einschließlich Inspektionen vor Ort, durch den System-Kunden oder einen von ihm beauftragten Prüfer zulassen und unterstützen muss, um die Überprüfung der Einhaltung der in Art. 28 DS-GVO und in diesem Katalog enthaltenen Pflichten des System-Anbieters zu gewährleisten.

Erläuterung

Um die Einhaltung der in diesem Katalog und sich unmittelbar aus Art. 28 DS-GVO ergebenden Pflichten zu gewährleisten und zu überprüfen, muss der Verantwortliche, bzw. der System-Kunde, in der Lage sein, die Einhaltung der Verpflichtungen selbständig zu überprüfen oder durch Dritte überprüfen zu lassen. Ein vertraglicher – und somit notfalls einklagbarer – Anspruch auf Überprüfung und Unterstützung bei der Überprüfung der Einhaltung dieser Verpflichtungen stärkt die Position des Verantwortlichen in dieser Aufgabe und gewährleistet damit mittelbar die Durchsetzung eines hohen Schutzniveaus für die personenbezogenen Daten der System-Nutzer (s.a. Nr. 11).

Umsetzungshinweis

„Der Vertrag muss Einzelheiten darüber enthalten, wie oft und auf welche Weise der Informationsfluss zwischen dem Auftragsverarbeiter und dem Verantwortlichen stattfinden sollte, damit der Verantwortliche umfassend über die Einzelheiten der Verarbeitung informiert ist, die für den Nachweis der Einhaltung der in Artikel 28 DS-GVO festgelegten Pflichten relevant sind. So können beispielsweise die maßgeblichen Teile des Verzeichnisses von Verarbeitungstätigkeiten des Auftragsverarbeiters an den Verantwortlichen weitergegeben werden. Der Auftragsverarbeiter sollte alle Informationen darüber bereitstellen, wie die Verarbeitungstätigkeit im Auftrag des Verantwortlichen durchgeführt wird. Diese Informationen sollten folgende Angaben umfassen: Funktionsweise der verwendeten Systeme, Sicherheitsmaßnahmen, Gewährleistung der Speicher-/ Aufbewahrungs-pflichten, Speicherort der Daten, Datenübermittlungen, Personen, die Zugriff auf die Daten haben, Empfänger der Daten, eingesetzte Unterauftragsverarbeiter usw.“[9]

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Ziffer 7.6 Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“

[9] EDSA, Leitlinien 07/2020, Rn. 143.

- ISO/IEC 27701:2025 Ziff. B.2.2.6 Kundenverpflichtungen

Kapitel II: Pflichten des System-Anbieters

Nr. 2 – Datenschutz-Managementsystem

Nr. 2.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten
(Art. 37 bis 39 DS-GVO i.V.m. dem nationalen Recht)

Kriterium

1) Der System-Anbieter benennt einen Datenschutzbeauftragten, wenn es sich bei ihm um eine Behörde oder eine öffentliche Stelle handelt.

2) Der System-Anbieter benennt einen Datenschutzbeauftragten, wenn seine Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

3) Der System-Anbieter benennt einen Datenschutzbeauftragten, wenn seine Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht.

4) Der System-Anbieter benennt einen Datenschutzbeauftragten, soweit das nationale Recht dies verlangt.

5) Der System-Anbieter benennt den Datenschutzbeauftragten aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben.

6) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte unmittelbar der höchsten Managementebene berichtet.

7) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.

8) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

9) Der System-Anbieter stellt die Anerkennung der Person und Funktion des Datenschutzbeauftragten im Organisationsgefüge sicher und unterstützt ihn bei seinen Aufgaben, insbesondere mit angemessenen Ressourcen.

10) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte seinen Aufgaben nach Art. 39 Abs. 1 DS-GVO im angemessenen Umfang nachkommen kann, einschließlich der Unterrichtung und Beratung, der Überwachung der Einhaltung der Vorschriften sowie der Zusammenarbeit mit der Aufsichtsbehörde und der Funktion als Kontaktstelle für diese.

11) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben auch über das Ende seines Rechtsverhältnisses mit dem System-Anbieter hinaus an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Dies umfasst insbesondere die Pflicht des Datenschutzbeauftragten zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen, soweit er nicht davon durch die betroffene Person befreit wird.

12) Der System-Anbieter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

13) Ist der Datenschutzbeauftragte kein Beschäftigter des System-Anbieters, stellt der System-Anbieter sicher, dass der Datenschutzbeauftragte einfach erreichbar ist. Gleiches gilt,

wenn der Datenschutzbeauftragte für mehrere Einrichtungen, etwa in Konzernstrukturen, zuständig ist.

14) Der System-Anbieter stellt sicher, dass andere Aufgaben oder Pflichten des Datenschutzbeauftragten zu keinem Interessenkonflikt mit seiner Tätigkeit als Datenschutzbeauftragten führen.

Erläuterung

Der System-Anbieter muss gemäß Art. 37 Abs. 1 lit. a DS-GVO einen Datenschutzbeauftragten benennen, wenn es sich bei ihm um eine Behörde oder eine öffentliche Stelle handelt (mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln). Dies wird allenfalls in besonderen Ausnahmefällen der Fall sein.

Der System-Anbieter muss gemäß Art. 37 Abs. 1 lit. b DS-GVO einen Datenschutzbeauftragten benennen, wenn seine Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Der Begriff der „Kerntätigkeit" wird in EG 97 DS-GVO dahingehend präzisiert, dass er sich auf die Haupttätigkeit eines Unternehmens und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit bezieht. Eine Haupttätigkeit ist gegeben, wenn die Datenverarbeitung bei der Erreichung der Unternehmensziele eine wesentliche Rolle spielt oder damit untrennbar verbunden ist.[10] Ziel der Anbieter schulischer Informationssysteme ist es regelmäßig, Wissen an Schülerinnen und Schüler zu vermitteln (z. B. durch Bereitstellung digitaler Lehrbücher und Lernanwendungen) oder dabei unterstützend tätig zu werden (z. B. durch Bereitstellung von Serverlösungen oder Log-in-Anwendungen). Die damit einhergehende Verarbeitung personenbezogener Daten von Schülerinnen und Schülern spielt damit eine wesentliche Rolle zur Erreichung dieser Ziele bzw. ist damit untrennbar verbunden, sodass es sich um eine Kerntätigkeit i.S.v. Art. 37 Abs. 1 lit. b DS-GVO handelt.

Art. 37 Abs. 1 lit. b DS-GVO ist einschlägig, wenn die Verarbeitungsvorgänge, die der Kerntätigkeit des System-Anbieters zuzurechnen sind, aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Überwachung i.d.S. meint Beobachten[11] (engl.: „monitoring"), also die Beobachtung des Verhaltens betroffener Personen.[12] Im Kontext schulischer Informationssysteme kann eine solche Überwachung z. B. gegeben sein, wenn beobachtet – d.h. erfasst und festgehalten – wird, wie häufig und in welchem Tempo Schülerinnen und Schüler eine Lernanwendung benutzen und wie (erfolgreich) sie bestimmte Aufgaben oder Tests lösen. Von einer regelmäßigen und systematischen Überwachung kann dabei gesprochen werden, wenn die Überwachung (also das Beobachten) nicht nur gelegentlich erfolgt und auf einem gezielten und planmäßigen Vorgehen beruht.[13] Ob sie umfangreich ist, bestimmt sich u.a. nach der Zahl der betroffenen Personen, der Dauer und dem Datenvolumen.[14]

Verarbeitungsvorgänge, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine derartige Überwachung erforderlich machen, können z. B. vorliegen, wenn schulische Informationssysteme automatisiert Lernfortschritte erfassen, an den Lernstand angepasste Lerninhalte vorschlagen (adaptives Lernen) oder gelöste Aufgaben und Tests bewerten, soweit dabei das Verhalten der Schülerinnen und Schüler durchgehend und planmäßig beobachtet wird. Anders wäre dies ggf. einzuschätzen, wenn es sich um eine einmalige Ergebnisermittlung bei einem Test handelt. Auch wird z. B. die Bereitstellung eines digitalen Schulbuches i.d.R. nicht mit einer Überwachung i.S.v. Art. 37 Abs. 1 lit. b DS-GVO einhergehen.

Der System-Anbieter muss gemäß Art. 37 Abs. 1 lit. c DS-GVO einen Datenschutzbeauftragten benennen, wenn seine Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht.

[10] Simitis/Hornung/Spiecker gen. Döhmann/*Drewes*, Art. 37 DS-GVO Rn. 16; Art.-29-Gruppe, WP 243 Rev.01, S. 8.
[11] BeckOK Datenschutzrecht/*Moos*, Art. 37 DS-GVO Rn. 28.
[12] Art.-29-Gruppe, WP 243 Rev.01, S. 10.
[13] Simitis/Hornung/Spiecker gen. Döhmann/*Drewes*, Art. 37 DS-GVO Rn. 27; s.a. Art.-29-Gruppe, WP 243 Rev.01, S. 10.
[14] S. Art.-29-Gruppe, WP 243 Rev.01, S. 9.

Eine Kerntätigkeit i.d.S. liegt vor, wenn die Datenverarbeitung bei der Erreichung der Unternehmensziele eine wesentliche Rolle spielt oder damit untrennbar verbunden ist (s.o. zu Art. 37 Abs. 1 lit. b DS-GVO). Zu den besonderen Kategorien personenbezogener Daten gehören gemäß Art. 9 Abs. 1 DS-GVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Daten i.S.v. Art. 10 DS-GVO wird im schulischen Kontext hingegen – wenn überhaupt – nur eine untergeordnete Bedeutung zukommen. Von einer umfangreichen Verarbeitung i.S.v. Art. 37 Abs. 1 lit. c DS-GVO kann u.a. ausgegangen werden, wenn eine große Zahl an Personen betroffen ist, wenn zahlreiche Daten verarbeitet werden und/oder wenn die Verarbeitung eine erheblich zeitliche oder geografische Ausdehnung aufweist.[15]

Zudem kann die Benennung eines Datenschutzbeauftragten nach nationalem Recht erforderlich sein. Dies bestimmt sich nach § 38 Abs. 1 BDSG (i.V.m. Art. 37 Abs. 4 S. 1 DS-GVO) und ist für die folgenden Fälle vorgesehen:

- wenn der System-Anbieter in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt,
- wenn der System-Anbieter Datenverarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, oder
- wenn der System-Anbieter personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

Der Datenschutzbeauftragte kann Beschäftigter des System-Anbieters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen (externer Datenschutzbeauftragter).

Der System-Anbieter muss den Datenschutzbeauftragten sorgfältig auswählen, ausstatten, schützen und ihm in der Betriebsorganisation einen gebührenden Platz zuweisen. Art. 38 Abs. 5 DS-GVO bestimmt, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Die Norm ist so auszulegen, dass diese Pflicht für den Datenschutzbeauftragten auch über das Ende seines Rechtsverhältnisses mit dem System-Anbieter hinaus fort gilt.

Der Datenschutzbeauftragte muss seinen gesetzlichen Pflichten in Bezug auf alle durchgeführten Verarbeitungsvorgänge nachkommen, unabhängig davon, ob der System-Anbieter als Auftragsverarbeiter oder Verantwortlicher der Datenverarbeitung agiert.

Umsetzungshinweis

Der System-Anbieter sollte dokumentieren, ob ein Datenschutzbeauftragter benannt werden muss. Wird kein Datenschutzbeauftragter benannt, sollten die Gründe hierfür ebenfalls dokumentiert werden.

Der System-Anbieter sollte eine schriftliche Dokumentation der für das jeweilige schulische Informationssystem eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister) und eine möglichst exakte Beschreibung der Gesamtheit der getroffenen TOM führen (z. B. in einem Datensicherheitskonzept) und dem Datenschutzbeauftragten sowie (auf Anfrage) der Aufsichtsbehörde zugänglich machen.

Der System-Anbieter sollte TOM treffen, um sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Zur Einbeziehung des Datenschutzbeauftragten kann beispielsweise ein Ticketsystem verwendet werden.

Ist der Datenschutzbeauftragte bei einem anderen Unternehmen beschäftigt (externer Datenschutzbeauftragter des System-Anbieters) oder gleichzeitig Datenschutzbeauftragter anderer Unternehmen, gilt seine Weisungsfreiheit auch gegenüber seinem Arbeitgeber und seinen anderen

[15] Art.-29-Gruppe, WP 243 Rev.01, S. 9 f.

Auftraggebern. Die Anforderung der Abwesenheit von Interessenskonflikten ist primär eine Benennungsvoraussetzung und in sekundärer Hinsicht eine Organisationspflicht des System-Anbieters. Der System-Anbieter weist dem Datenschutzbeauftragten keine zusätzlichen Aufgaben zu, die ihn in einen Interessenskonflikt bringen könnten. Interessenskonflikte sind im Rahmen folgender Tätigkeiten anzunehmen: Tätigkeiten, im Rahmen derer der Datenschutzbeauftragte sich selbst kontrollieren müsste, z. B. Stellung als Geschäftsführer, IT- oder Personalabteilungsleiter, wirtschaftliche Interessen des Datenschutzbeauftragten am Unternehmenserfolg oder zu große Nähe zur benennenden Stelle.

Die Geheimhaltungs- oder Vertraulichkeitspflicht des Datenschutzbeauftragten umfasst alle diesbezüglich relevanten Informationen. Dies sollte auch aus der Benennungsurkunde hervorgehen. Auch gegenüber der ihn benennenden Stelle ist der Datenschutzbeauftragte zur umfassenden Verschwiegenheit verpflichtet. Das Kriterium fördert das Gewährleistungsziel der Vertraulichkeit (SDM C1.4).

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 243 Rev.01 Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)
- DSK, Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
- ISO/IEC 27002:2022 Ziff. 5.2 Informationssicherheitsrollen und -verantwortlichkeiten
- ISO/IEC 27002:2022 Ziff. 5.3 Aufgabentrennung
- ISO/IEC 27701:2025 Ziff. B.3.4 Informationssicherheitsrollen und -verantwortlichkeiten

Nr. 2.2 – Meldung von Verletzungen des Schutzes personenbezogener Daten

(Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass er dem System-Kunden Verletzungen des Schutzes personenbezogener Daten und deren Ausmaß unverzüglich meldet.

2) Der System-Anbieter bestimmt, wer intern zuständig ist, über die Meldung an den System-Kunden zu entscheiden und diese vorzunehmen. Die zuständigen Stellen sind für Mitarbeitende und Subauftragsverarbeiter in einer Weise erreichbar, dass Meldungen über etwaige Verstöße zeitnah entgegengenommen und bearbeitet werden können.

3) Die zuständigen Stellen verfügen über ausreichend Ressourcen, um eine rasche Bearbeitung von Meldungen sicher zu stellen. Die Mitarbeitenden in den zuständigen Stellen sind ausreichend geschult, um Verstöße beurteilen und eine Folgenabschätzung durchführen zu können.

4) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte (sofern ein solcher benannt wurde) über Verletzungen des Schutzes personenbezogener Daten sowie den diesbezüglichen Umgang unverzüglich informiert wird, sollte der Datenschutzbeauftragte nicht zuständige Stelle im Sinne des Abs. 2 sein.

Erläuterung

Der System-Anbieter ist nach Art. 33 Abs. 2 DS-GVO zur unverzüglichen Meldung von Verletzungen des Schutzes personenbezogener Daten an den System-Kunden verpflichtet, damit dieser seiner Meldepflicht gegenüber der Aufsichtsbehörde aus Art. 33 Abs. 1 DS-GVO und seiner Unterrichtungspflicht gegenüber den betroffenen Personen aus Art. 34 Abs. 1 DS-GVO nachkommen kann. Diese Pflicht bezieht sich auch auf Verstöße von Subauftragnehmern in der gesamten Subauftragsverarbeiterkette. Das Kriterium fördert die Gewährleistungsziele der Integrität und Transparenz (SDM C1.3 und C1.6).

Eine Verletzung des Schutzes personenbezogener Daten ist gemäß Art. 3 Nr. 12 DS-GVO eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Umsetzungshinweis

Der System-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die Meldung von Verletzungen des Schutzes personenbezogener Daten kann über geeignete Informationssysteme innerhalb des Systems wie über Nachrichtensysteme oder Newsmeldungen geschehen. Sie sollte in das Incident- und Troubleshooting-Management des System-Anbieters integriert werden, um eine rasche Bearbeitung zu ermöglichen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Klausel 9 im Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- EDSA, Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO
- ISO/IEC 27002:2022 Ziff. 5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- ISO/IEC 27002:2022 Ziff. 5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
- ISO/IEC 27002:2022 Ziff. 5.26 Reaktion auf Informationssicherheitsvorfälle
- ISO/IEC 27701:2025 Ziff. B.3.11 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- ISO/IEC 27701:2025 Ziff. B.3.12 Reaktion auf Informationssicherheitsvorfälle

Nr. 2.3 – Führen eines Verzeichnisses von Verarbeitungstätigkeiten
(Art. 30 Abs. 2 bis 5 DS-GVO)

Kriterium

1) Der System-Anbieter führt ein Verzeichnis von Verarbeitungstätigkeiten.
2) Der System-Anbieter führt in dem Verzeichnis von Verarbeitungstätigkeiten alle Kategorien von Verarbeitungen auf, die er im Auftrag von System-Kunden vornimmt. Das Verzeichnis enthält die in Art. 30 Abs. 2 lit. a bis d DS-GVO aufgelisteten Inhalte.
3) Der System-Anbieter verfügt über einen Prozess, der sicherstellt, dass die Angaben nach Art. 30 Abs. 2 lit. a bis d DS-GVO aktualisiert werden, wenn im Auftrag durchgeführte Verarbeitungstätigkeiten eingeführt werden, wegfallen oder sich ändern, sowie wenn Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, hinzukommen, wegfallen oder sich bei bestehenden Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird, Angaben nach Art. 30 Abs. 2 lit. a bis d DS-GVO ändern.
4) Das Verzeichnis von Verarbeitungstätigkeiten ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Die Aufbewahrungs- oder Speicherorte müssen dem System-Anbieter bekannt sein.
5) Das Verzeichnis von Verarbeitungstätigkeiten ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Der System-Anbieter verfügt über Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden und regelt hierfür die internen Zuständigkeiten.
6) Ist der System-Anbieter zur Benennung eines Vertreters (i.S.v. Art. 4 Nr. 17 i.V.m. Art. 27 DS-GVO) verpflichtet, stellt er sicher, dass auch der Vertreter ein Verzeichnis von Verarbeitungstätigkeiten führt und die Kriterien nach Abs. 1 bis 5 einhält.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM C1.6).

Der System-Anbieter hat als Auftragsverarbeiter gemäß Art. 30 Abs. 2 DS-GVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Art. 30 Abs. 5 DS-GVO sieht eine Ausnahme von dieser Pflicht vor, wenn der System-Anbieter weniger als 250 Mitarbeitende beschäftigt. Diese Ausnahme ist allerdings nicht anwendbar, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder wenn eine Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO bzw. von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.v. Art. 10 DS-GVO erfolgt.

Anbieter schulischer Informationssysteme verarbeiten personenbezogene Daten nicht nur gelegentlich (also nur „hin und wieder", „unregelmäßig" oder „sporadisch"[16]), sondern – und sei es z. B. auch nur in Form von Stammdaten oder pseudonymen Schülerkennungen – fortlaufend und regelmäßig. Daher ist die Ausnahme nach Art. 30 Abs. 5 DS-GVO auf Anbieter schulischer Informationssysteme nicht anwendbar. Zudem ist zu berücksichtigen, dass die Beantragung und Durchführung der Zertifizierung einen gewissen Dokumentationsaufwand mit sich bringen, wofür das Verzeichnis von Verarbeitungstätigkeiten die Grundlage sein kann.

Nach Art. 30 Abs. 2 DS-GVO hat auch der Vertreter des System-Anbieters (i.S.v. Art. 4 Nr. 17 i.V.m. Art. 27 DS-GVO) ein Verzeichnis von Verarbeitungstätigkeiten zu führen, wenn ein solcher benannt ist (s. Nr. 14.2). Der System-Anbieter unterstützt zudem den System-Kunden bei der Führung seines Verzeichnisses von Verarbeitungstätigkeiten (Nr. 8).

Umsetzungshinweis

Für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten kann auch auf bestehende Datenflussdiagramme zurückgegriffen werden.

Das Verzeichnis von Verarbeitungstätigkeiten kann für alle Dokumentationspflichten als Nachweis oder Nachweisbekräftigung herangezogen werden. Dieses Verzeichnis ist jedoch nicht öffentlich und richtet sich nicht an betroffene Personen, sondern ist ausschließlich nach innen und auf das Verhältnis zur Aufsichtsbehörde gerichtet.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
- DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO
- ISO/IEC 27701:2025 Ziff. B.2.2.7 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten

Zu Mustern von Verzeichnissen von Verarbeitungstätigkeiten s. LDI NRW, https://www.ldi.nrw.de/datenschutz/verwaltung/verarbeitungsverzeichnis.

Nr. 2.4 - Änderungen des Datenverarbeitungsortes
(Art. 28 Abs. 3 DS-GVO)

Kriterium

> Der System-Anbieter informiert den System-Kunden (also dessen befugte Mitarbeitende) unverzüglich, wenn die Datenverarbeitung während des Geltungszeitraums der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung aus der EU bzw. dem EWR in ein Drittland verlegt wird.

Umsetzungshinweis

Bei Massengeschäften sollte ein Kommunikationsprozess, möglichst unterstützt durch eine automatisierte Funktion innerhalb des schulischen Informationssystems, eingerichtet werden, wodurch der System-Kunde bzw. seine Mitarbeitenden von der Verlegung der der Datenverarbeitung (z. B. Verlagerung der Server) automatisch Kenntnis erlangt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

[16] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 30 DS-GVO Rn. 46.

- ISO/IEC 27701:2025 Ziff. B.2.5.2 Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen
- ISO/IEC 27701:2025 Ziff. B.2.5.3 Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können

Nr. 2.5 – Einrichtung eines internen Kontrollsystems zur Einhaltung der DS-GVO
(Art. 24 und 28 DS-GVO)

Kriterium

1) Der System-Anbieter verfügt über einen Prozess zur regelmäßigen Überprüfung (mindestens jährlich sowie bei wesentlichen Veränderungen) der Einhaltung und Umsetzung der Anforderungen der DS-GVO. Hierfür legt der System-Anbieter Kontrollverfahren und Zuständigkeiten fest und handelt bei Befunden mit präventiven und korrektiven Maßnahmen.
2) Der Prozess stellt sicher, dass die Anforderungen der DS-GVO auch bei der (Weiter-)Entwicklung oder Änderung des schulischen Informationssystems weiterhin eingehalten werden.

Erläuterungen

Der System-Anbieter hat sicherzustellen, dass die Maßnahmen zur Erfüllung der datenschutzrechtlichen Anforderungen der DS-GVO nicht nur einmalig implementiert werden, sondern fortlaufend aufrechterhalten werden.

Umsetzungshinweis

Der System-Anbieter sollte vor allem die internen Audits des Datenschutzbeauftragten (sofern ein solcher benannt wurde) zu Datenschutzfragen heranziehen.

Der System-Anbieter sollte die Wirksamkeit der internen Kontrollaktivitäten regelmäßig überprüfen. Dazu gilt es zunächst zu definieren, wie die Wirksamkeit der internen Kontrollaktivitäten gemessen werden kann. Es wird empfohlen, ein standardisiertes Vorgehensmodell (z. B. ITIL oder COBIT) für die IT-Prozesse des angebotenen schulischen Informationssystems zu definieren und einzuhalten. Wird ein interner Prüfer/Auditor eingesetzt, sollte er über eine geeignete Qualifikation verfügen sowie objektiv und unparteiisch und nicht an der Entwicklung des schulischen Informationssystems beteiligt sein.

Auf die folgenden Umsetzungshinweise wird hingewiesen.

- SDM, Abschnitt D4.4.3 Check: Kontrollieren / Prüfen / Beurteilen
- ISO/IEC 27002:2022 Ziff. 5.35 Unabhängige Überprüfung der Informationssicherheit
- ISO/IEC 27002:2022 Ziff. 5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
- ISO/IEC 27701:2025 Ziff. B.3.15 Unabhängige Überprüfung der Informationssicherheit

Nr. 2.6 – Auswahl und Einsatz geeigneter Personen
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c, e und f, UAbs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter betraut nur Mitarbeitende mit der Durchführung von Verarbeitungsvorgängen, die fachlich für die Erfüllung ihrer jeweiligen Aufgaben befähigt sind und sowohl im Datenschutz als auch in der Datensicherheit sensibilisiert und geschult sind.
2) Der System-Anbieter stellt sicher, dass Mitarbeitende fortlaufend im Themenfeld Datenschutz und Datensicherheit geschult werden. Die Schulungen müssen insbesondere sicherstellen, dass die Mitarbeitenden grundlegende Kenntnis von den aktuellen datenschutzrechtlichen Vorschriften erlangen, die für das von dem System-Anbieter angebo-

tene schulische Informationssystem maßgeblich sind. Dies umfasst auch die Kenntnisnahme der Materialien, die von den zuständigen Aufsichtsbehörden zum Datenschutz an Schulen bereitgestellt werden.

Erläuterungen

Gemäß Art. 28 Abs. 1 DS-GVO arbeitet der Verantwortliche (hier der System-Kunde) nur mit einem Auftragsverarbeiter (hier dem System-Anbieter) zusammen, der hinreichende Garantien dafür bietet, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Zudem hat der System-Anbieter als Auftragsverarbeiter den System-Kunden als Verantwortlichen gemäß Art. 28 Abs. 3 UAbs. 2 DS-GVO unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt (Nr. 5.1).

Beim System-Anbieter müssen daher Kenntnisse vom einschlägigen Datenschutz- und Datensicherheitsrecht vorhanden sein (s.a. EG 81 Satz 1 DS-GVO: „Fachwissen, Zuverlässigkeit und Ressourcen"). Andernfalls darf er nicht als Auftragsverarbeiter herangezogen werden. Dies wiederum bedingt, dass der System-Anbieter über Mitarbeitende verfügt, die ein ausreichendes Fachwissen im Bereich des Datenschutzes und der Datensicherheit aufweisen.[17]

Das Kriterium steht in enger Verbindung mit dem Kriterium Nr. 2.1, da der Datenschutzbeauftragte (sofern ein solcher benannt wurde) für die Sensibilisierung und Schulung der Mitarbeitenden zuständig ist und die diesbezüglichen Überprüfungen vornimmt.

Umsetzungshinweis

Um die fachliche Kompetenz der Mitarbeitenden zu erhalten, sollte der System-Anbieter regelmäßige Mitarbeitendenschulungen (ca. einmal pro Jahr) zu datenschutzrechtlichen und datensicherheitstechnischen Themen durchführen – auch zur konkreten Technik des schulischen Informationssystems. Die Schulung von Mitarbeitenden obliegt dem Datenschutzbeauftragten (sofern ein solcher benannt wurde).

Die Schulungen sollten Kenntnisse der schuldatenschutzrechtlichen Vorschriften der Länder vermitteln und die Materialien der Aufsichtsbehörden zum Schuldatenschutz (Stellungnahmen, Orientierungshilfen etc.) berücksichtigen. Exemplarisch wird auf die folgenden Materialien hingewiesen:

- Hessen: https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/datenschutzrechtliche-pflichten-einer-schule-nach-der-ds-gvo
- Nordrhein-Westfalen: https://www.ldi.nrw.de/digitaler-unterricht-schulen-der-grundstein-ist-gelegt
- Rheinland-Pfalz: https://www.datenschutz.rlp.de/themen/datenschutz-in-der-schule-faq

Auf die folgenden Umsetzungshinweise wird hingewiesen.

- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln"
- ISO/IEC 27002:2022 Ziff. 6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
- ISO/IEC 27701:2025 Ziff. B.3.17 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Nr. 2.7 – Kosten und Gebühren Unterstützung des System-Kunden
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e, f und h DS-GVO)

Kriterium

Wenn der System-Anbieter gegenüber dem System-Kunden Kosten und Gebühren für die Zurverfügungstellung der Informationen und die Durchführung der Überprüfungen nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO (s. Nr. 1.10) sowie für Unterstützungshandlungen

[17] S. Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 39.

nach Nr. 7, Nr. 8, Nr. 9 oder Nr. 10 geltend macht, muss er diese im Einzelfall transparent und nachvollziehbar darlegen.

Erläuterung

Der System-Anbieter ist nicht verpflichtet, gegenüber dem System-Kunden Kosten und Gebühren für die Zurverfügungstellung der Informationen und die Durchführung der Überprüfungen nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO (s. Nr. 1.10) sowie für Unterstützungshandlungen nach Nr. 7, Nr. 8, Nr. 9 oder Nr. 10 geltend zu machen. Dieses Kriterium soll daran nichts ändern. Es enthält aber die Vorgabe, dass die Kosten und Gebühren – falls sie geltend gemacht werden – transparent und nachvollziehbar sein müssen. Diese Transparenz sollte aufgrund von Wettbewerbseffekten im Regelfall dazu führen, dass Kosten nicht unangemessen oder unverhältnismäßig hoch sind.

Die Frage der Kostenverteilung zwischen dem Verantwortlichen und dem Auftragsverarbeiter im Zusammenhang mit Überprüfungen nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO (s. Nr. 1.10) fällt nach den Leitlinien des EDSA nicht unter die DS-GVO und unterliegt wirtschaftlichen Erwägungen. Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO verlangt nach Auffassung des EDSA jedoch, „dass der Vertrag den Auftragsverarbeiter verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, und dass er verpflichtet ist, Überprüfungen einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen vom Verantwortlichen beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen. In der Praxis bedeutet dies, dass die Vertragsparteien keine Klauseln vereinbaren sollten, die die Zahlung eindeutig unangemessener oder unverhältnismäßig hoher Kosten und Gebühren zum Gegenstand haben und dadurch eine abschreckende Wirkung auf eine der Parteien ausüben würden. Solche Klauseln würden in der Tat bedeuten, dass die in Artikel 28 Absatz 3 Buchstabe h festgelegten Rechte und Pflichten in der Praxis nie ausgeübt würden und rein theoretisch wären, obwohl sie integraler Bestandteil der Datenschutzgarantien nach Artikel 28 DS-GVO sind.“[18]

Umsetzungshinweis

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“

Nr. 3 – Gewährleistung der Datensicherheit durch risikoangemessene TOM

Erläuterung

Der Verantwortliche (hier der System-Kunde) und der Auftragsverarbeiter (hier der System-Anbieter) haben gemäß Art. 32 DS-GVO geeignete TOM vorzusehen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Es handelt sich mithin um eine Pflicht, die sich direkt (auch) an den System-Anbieter richtet. Dies wiederholt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c DS-GVO (s. Nr. 1.7 Abs. 1).[19] Zudem ist der System-Anbieter gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DS-GVO verpflichtet, den System-Kunden bei der Einhaltung von dessen Pflichten nach Art. 32 DS-GVO zu unterstützen. Dies wird in Nr. 3 abgebildet.

Gemäß Art. 5 Abs. 1 lit. f i.V.m. Art. 32 DS-GVO ist ein angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die besonderen schulischen Gegebenheiten (z. B. Verarbeitung der Daten Minderjähriger) und die Risikobewertung (z. B. Verarbeitung von besonderen Kategorien personenbezogener Daten oder Kontaktdaten von Schülerinnen und Schülern) sind ebenfalls zu berücksichtigen.

[18] EDSA, Leitlinien 07/2020, Rn. 145.
[19] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 68.

Nr. 3.1 – Datensicherheitskonzept
(Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter führt eine Risikoanalyse der Verarbeitungsvorgänge des schulischen Informationssystems in Bezug auf die Datensicherheit auf Grundlage des Risikobewertungskonzepts[20] oder eines anderen, mindestens gleichwertigen, Verfahrens zur Risikobewertung durch und muss dabei auf die besonderen schulischen Gegebenheiten Rücksicht nehmen. Bei der Risikoanalyse sind der Stand der Technik, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken der Verarbeitungsvorgänge, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, zu berücksichtigen.

2) Auf Grundlage der Risikoanalyse erstellt der System-Anbieter ein fortzuschreibendes Datensicherheitskonzept, das TOM vorsieht, um bestehende Risiken zu minimieren. Hierzu zählen insbesondere Maßnahmen zur Pseudonymisierung, Anonymisierung und Verschlüsselung personenbezogener Daten. In dem Datensicherheitskonzept stellt der System-Anbieter dar, welche TOM er umgesetzt hat, um bestehende Risiken einzudämmen, und bestimmt, wer für die Umsetzung der TOM zuständig ist. Der System-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen TOM zu gelangen.

3) Das Datensicherheitskonzept ist schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann.

4) Das Datensicherheitskonzept ist in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren. Entsprechend der Aktualisierung sind die TOM anzupassen.

5) Das Datensicherheitskonzept beschreibt, welche Verarbeitungsvorgänge vom System-Anbieter durchgeführt werden und welche Verarbeitungsvorgänge ggf. von Subauftragsverarbeitern durchgeführt werden.

6) Das Datensicherheitskonzept beschreibt, welche Verarbeitungsvorgänge vom System-Anbieter selbst durchgeführt werden und welche der Verantwortung des System-Kunden unterliegen.

7) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des System-Kunden verlangt, sind diese dem System-Kunden vor dem Beginn der Datenverarbeitung oder vor Änderungen schriftlich, was auch in einem elektronischen Format erfolgen kann, mitzuteilen und so zu beschreiben, dass eine Umsetzung durch den System-Kunden möglich ist.

8) Die geforderten Angaben können, müssen aber nicht in einem einheitlichen Dokument zum Datensicherheitskonzept zusammengefasst sein. Es darf sich auch um eine Sammlung von Dokumenten handeln.

Erläuterung

Ein Datensicherheitskonzept dokumentiert u.a. Schutzprinzipien, identifizierte Risiken und festgelegte TOM zum Schutz der verarbeiteten Daten.

Der System-Anbieter hat gemäß Art. 32 Abs. 1 DS-GVO risikoangemessene TOM festzulegen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und eine Verletzung der Rechte und Freiheiten von natürlichen Personen (Schülerinnen und Schüler, Lehrkräfte, Erziehungsberechtigte etc.) nach Möglichkeit zu verhindern. Insbesondere hat er Risiken mit Blick auf unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten auszuschließen oder zu minimieren.

Hierzu hat er bestehende Risiken zu ermitteln und zu analysieren, was auf Grundlage des Risikobewertungskonzepts (siehe Begleitdokument) oder eines mindestens vergleichbaren Verfahrens erfolgen kann. Bei der Festlegung der konkreten Maßnahmen berücksichtigt er nicht nur die Modalitäten der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Schadens, sondern auch den Stand der Technik sowie die Implementierungskosten der Maßnahmen. Die dabei

[20] Siehe Begleitdokument Risikobewertungskonzept.

getroffenen Abwägungen müssen aus dem Datensicherheitskonzept ersichtlich sein. Ist dem System-Anbieter bekannt, dass eine beim System-Kunden durchgeführte Datenschutz-Folgenabschätzung ein hohes Risiko der Verarbeitung offenbart hat, hat er auch dies bei der Festlegung konkreter Maßnahmen zu berücksichtigen.

Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.[21]

An die Schulen bzw. die Schulleitung gerichtete Vorgaben zur Datensicherheit finden sich vereinzelt im jeweiligen Landesrecht. So ist die Schule z. B. in Hessen (§ 6 SchDSV-HE) und in Mecklenburg-Vorpommern (§ 6 SchulDSVO M-V) zur Erstellung eines IT-Sicherheitskonzepts verpflichtet.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- DSK, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen
- SDM-Baustein 41 „Planen und Spezifizieren“
- BSI, IT Grundschutz Kompendium (insbesondere CON.2 Datenschutz)
- ISO 31000:2018 Risikomanagement - Leitlinien
- IEC 31010:2019 Risikomanagement - Verfahren zur Risikobeurteilung
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung

Nr. 3.2 – Schwachstellen- und Update-Management
(Art. 32 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter etabliert ein Verfahren zur Ermittlung von technischen Schwachstellen und sonstigen Sicherheitslücken im schulischen Informationssystem, das er fortlaufend anwendet. Er legt fest, wie häufig das schulische Informationssystem auf technische Schwachstellen und sonstige Sicherheitslücken untersucht wird. Art und Häufigkeit der Untersuchungen müssen dem unter Nr. 3.1 ermittelten Risiko angemessenen sein.

2) Der System-Anbieter richtet ein Verfahren ein, um ermittelte technische Schwachstellen und sonstige Sicherheitslücken in einem dem Risiko angemessenen Zeitrahmen zu beheben. Sollte ein angemessener Zeitraum nicht eingehalten werden können und wegen des hohen Risikos eine weitere Verarbeitung personenbezogener Daten über das System nicht haltbar sein, muss die Nutzung des Systems teilweise oder gänzlich durch den System-Anbieter unterbunden werden.

3) Das Verfahren nach Abs. 2 stellt insbesondere sicher, dass erforderliche Updates und Patches unverzüglich integriert werden, dass Updates und Patches vorher geplant, genehmigt, dokumentiert sowie geeignet getestet wurden und dass Rückfall-Lösungen vorhanden sind.

4) Der System-Anbieter richtet ein Verfahren zur Dokumentation der Updates und Patches ein.

5) Bei schwerwiegenden technischen Schwachstellen und sonstigen Sicherheitslücken stellt der System-Anbieter sicher, dass der System-Kunde über die Schwachstellen und Sicherheitslücken sowie die Updates und Patches informiert wird.

[21] S. zum Begriff auch das Glossar.

6) Der System-Anbieter stellt sicher, dass sich der System-Kunde über die Version des verwendeten schulischen Informationssystems informieren kann.

Erläuterung

Der System-Anbieter hat zur Einhaltung von Art. 32 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO Verfahren zur Ermittlung von technischen Schwachstellen und sonstigen Sicherheitslücken und deren Behebung – insbesondere durch Updates und Patches – vorzusehen.

Um dem System-Kunden die Möglichkeit zu geben, die Sicherheit des Systems und die Überprüfungsmaßnahmen des System-Anbieters zu überprüfen, sind entsprechende Transparenzmaßnahmen zu ergreifen.

Insbesondere bei Verwendung von Open-Source-Software (OSS, also quelloffener Software) muss der System-Anbieter gemeldete technische Schwachstellen und sonstiger Sicherheitslücken kontinuierlich überwachen (v.a. über CVE, https://www.cve.org/). Es muss ein Prozess eingerichtet werden, um die Relevanz neuer Meldungen über technische Schwachstellen und sonstige Sicherlücken zu bewerten und ggf. erforderliche Maßnahme zu ergreifen. Werden technische Schwachstellen und sonstige Sicherheitslücken bekannt (z. B. durch Hinweise zuständiger Behörde oder in CVE-Datenbanken), muss der System-Anbieter tätig werden.

Umsetzungshinweis

Untersuchungen des schulischen Informationssystems auf technische Schwachstellen und sonstige Sicherheitslücken sollten regelmäßig erfolgen. Grundsätzlich sollte die Behebung gefundener Schwachstellen und Sicherheitslücken unverzüglich erfolgen.

Für die Bestimmung der Schwere einer technischen Schwachstelle und sonstigen Sicherheitslücke kann z. B. das „Common Vulnerability Scoring System“ (CVSS) herangezogen werden.

Bei der Bereitstellung eines schulischen Informationssystems sollten Prozesse für ein sicheres Änderungs- und Release-Management etabliert werden. Im Rahmen dieser Prozesse sollte ein System-Anbieter u.a. eine dokumentierte Eignungsprüfung und einen Abnahmeprozess bei der (Weiter-)Entwicklung und Änderung (insbesondere Patches und System-Updates) an seinem System durchführen, um nachteilige Auswirkungen aufgrund der Änderungen zu vermeiden und die Konformität zur DS-GVO fortlaufend sicherzustellen. Die Geltungsbereiche, Rollen und Verbindlichkeiten im Rahmen des Änderungs- und Release-Managements sollten zwischen System-Anbieter und -Kunden klar definiert und aufeinander abgestimmt sein.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- BSI, IT Grundschutz Kompendium Elementare Gefährdungen, G 0.28 Software-Schwachstellen oder -Fehler
- BSI, IT Grundschutz Kompendium OPS Betrieb
- BSI, IT Grundschutz Kompendium DER Detektion und Reaktion
- ISO/IEC 27002:2022 Ziff. 8.8 Handhabung von technischen Schwachstellen
- ISO/IEC 27002:2022 Ziff. 8.32 Änderungssteuerung
- ISO/IEC 30111, Informationstechnik – IT-Sicherheitsverfahren – Prozesse für die Behandlung von Schwachstellen

Nr. 3.3 – Zutrittskontrolle und Schutz vor Schädigungen
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass Datenverarbeitungsanlagen[22] gegen den Zutritt[23] Unbefugter und gegen Schädigungen geschützt sind. Die TOM sind geeignet, den Zutritt Unbefugter sowie Schädigungen hinreichend sicher auszuschließen, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter und vor höherer Gewalt einschließt. Insbesondere ist eine risikoangemessene Authentifizierung beim Zutritt zu Datenverarbeitungsanlagen durchzuführen.

2) Der System-Anbieter verfügt bzgl. des Zutritts über ein Berechtigungskonzept. Zutrittsberechtigungen sind festzulegen und zu dokumentieren. Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

3) Zutritte und Zutrittsversuche zu Räumen, in denen sich Server oder ähnlich kritische Datenverarbeitungsanlagen befinden, werden protokolliert und sind nachträglich feststellbar. Die Protokolle werden befristet aufbewahrt.

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und 5 Abs. 1 lit. f DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen.

Zutritt i.S. dieses Kriteriums meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen. „Zutritt hat auch, wer durch Glaswände, offenstehende Türen oder Fenster Datenein- oder -ausgabegeräte beobachten und dabei Daten zur Kenntnis nehmen kann. Die Zutrittskontrolle verlangt daher auch eine optische Abschirmung. Unter Zutritt fällt auch die Möglichkeit, Datenein- oder -ausgabegeräte zu beeinflussen."[24]

Datenverarbeitungsanlagen i.S. dieses Kriteriums sind Geräte für die elektronische Verarbeitung von Daten (z. B. Server, Personal Computer oder Laptops einschließlich dazugehöriger Ein- und Ausgabegeräte), auf denen personenbezogene Daten im Zusammenhang mit dem schulischen Informationssystem des System-Anbieters verarbeitet werden.

Nach einer auf verschiedenen Gebieten des Unionsrechts entwickelten ständigen Rechtsprechung sind unter „höherer Gewalt" ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können.[25] Dies können – je nach Situation – etwa Naturkatastrophen (z. B. Erdbeben, Überschwemmungen oder Vulkanausbrüche), Kriege (inklusive Bürgerkriege) sowie Streiks und Sabotage sein.

Der System-Anbieter benötigt ein Berechtigungskonzept. Berechtigungen sind regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen (z. B. der Neueinstellung oder dem Ausscheiden eines Mitarbeitenden) zu prüfen und ggf. zu aktualisieren.

[22] Datenverarbeitungsanlagen i.S. dieses Kriteriums sind Geräte für die elektronische Verarbeitung von Daten (z. B. Server, Personal Computer oder Laptops einschließlich dazugehöriger Ein- und Ausgabegeräte), auf denen personenbezogene Daten im Zusammenhang mit dem schulischen Informationssystem des System-Anbieters verarbeitet werden.
[23] Zutritt i.S. dieses Kriteriums meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen.
[24] Simitis/*Ernestus*, § 9 BDSG Rn. 77.
[25] EuGH, Urt. v. 25.01.2017 – C-640/15, Rn. 53.

Umsetzungshinweis

Ein Schutz vor dem Zutritt Unbefugter kann durch zahlreiche Maßnahmen gewährleistet werden, etwa bauliche Maßnahmen, die Vergabe von Berechtigungen, Protokollierungen und Überwachungsmaßnahmen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2022 Ziff. 7 Physische Maßnahmen
- BSI, IT Grundschutz Kompendium: Infrastruktur, INF.1 Allgemeines Gebäude; INF.2 Rechenzentrum sowie Serverraum; INF.5 Raum sowie Schrank für technische Infrastruktur; INF.6 Datenträgerarchiv; INF.7 Büroarbeitsplatz; INF.8 Häuslicher Arbeitsplatz und INF.9 Mobiler Arbeitsplatz.

Nr. 3.4 – Zugangskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass Datenverarbeitungssysteme vor dem Zugang[26] Unbefugter geschützt sind. Dies gilt auch für Datenverarbeitungssysteme, die Sicherungskopien enthalten. Die TOM sind geeignet, den Zugang Unbefugter zu Datenverarbeitungssystemen hinreichend sicher auszuschließen, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter einschließt.

2) Die TOM nach Abs. 1 umfassen insbesondere Verfahren zur Vergabe, Aktualisierung und Aufhebung von Zugangsrechten und eine risikoangemessene Authentifizierung.

3) Der System-Anbieter verfügt bzgl. des Zugangs über ein Berechtigungskonzept. Zugangsberechtigungen sind festzulegen und zu dokumentieren. Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

4) Zugänge und Zugangsversuche zu Datenverarbeitungssystemen werden protokolliert und sind nachträglich feststellbar. Die Protokolle werden befristet aufbewahrt.

5) Der Zugang von Mitarbeitenden des System-Anbieters zu Datenverarbeitungssystemen über das Internet einschließlich der Fernadministration ist durch eine Multi-Faktor-Authentifizierung abzusichern und erfolgt über einen verschlüsselten Kommunikationskanal.

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele der Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen.

Zugang i.S. dieses Kriteriums meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem). Die Zugangskontrolle soll verhindern, dass Datenverarbeitungssysteme bzw. Systemkomponenten von Unbefugten genutzt werden können. Im Gegensatz dazu meint Zugriff (s. Nr. 3.5) den Zugriff auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems.

„Der Zugang von Mitarbeitenden des System-Anbieters zu Datenverarbeitungssystemen über das Internet“ i.S.v. Abs. 5 meint nicht den Fall, dass Schülerinnen und Schülern, Lehrkräfte sowie andere System-Nutzer über das Internet auf bestimmte Lernanwendungen (etc.) zugreifen, sondern dass Administratoren (etc.) auf das System selbst zugreifen.

[26] Zugang i.S. dieses Kriteriums meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem).

Der System-Anbieter benötigt ein Berechtigungskonzept. Berechtigungen sind regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen (z. B. der Neueinstellung oder dem Ausscheiden eines Mitarbeitenden) zu prüfen und ggf. zu aktualisieren.

Umsetzungshinweis

Eine Multi-Faktor-Authentifizierung kann z. B. durch die Pflicht zur Verwendung einer Zugangskarte (Besitz) mit anschließender Eingabe einer PIN (Wissen) umgesetzt werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung
- SDM-Baustein 43 „Protokollieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen, G.030 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- ISO/IEC 27002:2022 Ziff. 5.15 Zugangssteuerung
- ISO/IEC 27002:2022 Ziff. 5.18 Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.2 Privilegierte Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.3 Informationszugangsbeschränkung
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.9 Zugangsrechte
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung
- ISO/IEC 29146:2022 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung

Nr. 3.5 – Zugriffskontrolle

(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass personenbezogene Daten vor dem Zugriff[27] Unbefugter geschützt sind und Befugte nur im Rahmen ihrer Berechtigungen Zugriff auf personenbezogene Daten nehmen können. Dies gilt auch für Sicherungskopien, soweit sie personenbezogene Daten enthalten. Die TOM sind geeignet, den Zugriff Unbefugter auf personenbezogene Daten im schulischen Informationssystem hinreichend sicher auszuschließen, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter einschließt.

2) Die TOM nach Abs. 1 umfassen insbesondere eine risikoangemessene Authentifizierung. Administrative Zugriffe durch Mitarbeitende des System-Anbieters sind durch einen starken Authentisierungsmechanismus zu schützen.

3) Der System-Anbieter verfügt bzgl. des Zugriffs über ein Berechtigungskonzept. Zugriffsberechtigungen sind festzulegen und zu dokumentieren. Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

[27] Der Zugriff i.S. dieses Kriteriums meint den Zugriff auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems. Die Zugriffskontrolle soll sicherstellen, dass die zur Benutzung eines Datenverarbeitungssystems Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und auf die personenbezogenen Daten nicht unbefugt eingewirkt werden kann.

4) Der System-Anbieter ermöglicht es dem System-Kunden, verschiedene Berechtigungen festzulegen, um unbefugte Zugriffe auf personenbezogene Daten logisch auszuschließen.

5) Der System-Anbieter kontrolliert, also überwacht und bewertet, und protokolliert alle Zugriffe auf personenbezogene Daten. Zugriffe sind nachträglich feststellbar. Die Protokolle werden befristet aufbewahrt.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

Der Zugriff i.S. dieses Kriteriums meint den Zugriff auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems. Die Zugriffskontrolle soll sicherstellen, dass die zur Benutzung eines Datenverarbeitungssystems Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und auf die personenbezogenen Daten nicht unbefugt eingewirkt werden kann. Im Gegensatz dazu meint Zugang (s. Nr. 3.4) jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem).

Werden schulische Informationssysteme von Minderjährigen genutzt, sind altersgerechte Optionen für sichere Passwörter und altersgerechte Optionen für die Wiederherstellung von Zugriffsdaten bereitzustellen. Komplexe Passwörter sind zwar sicherer, für jüngere Kinder aber oft eine große Herausforderung. Hier kollidieren ggf. die Rechte des Kindes mit den allgemeinen Anforderungen des Datenschutzes und der Datensicherheit. Nach Möglichkeit sollten technische Lösungen wie Passphrasen implementiert werden (s.a. Nr. 3.6).

Der System-Anbieter benötigt ein Berechtigungskonzept. Berechtigungen sind regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen (z. B. der Neueinstellung oder dem Ausscheiden eines Mitarbeitenden) zu prüfen und ggf. zu aktualisieren.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung
- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 14 f.
- SDM-Baustein 43 „Protokollieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen, G.038 Missbrauch personenbezogener Daten
- BSI, IT Grundschutz Kompendium, ORP: Organisation und Personal, ORP.4 Identitäts- und Berechtigungsmanagement
- BSI, IT Grundschutz Kompendium, Konzepte und Vorgehensweisen, CON.10 Entwicklung von Webanwendungen, A2 Zugriffskontrolle bei Webanwendungen
- ISO/IEC 27002:2022 Ziff. 5.15 Zugangssteuerung
- ISO/IEC 27002:2022 Ziff. 5.18 Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.2 Privilegierte Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.3 Informationszugangsbeschränkung
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.9 Zugangsrechte

- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 3.6 – Informationen zu Passwörtern, Log-out und privaten Endgeräten
(Art. 32 Abs. 1 lit. b DS-GVO)

Kriterium

1) System-Anbieter von schulischen Informationssystemen haben System-Nutzer in einfacher und verständlicher Sprache auf Anforderungen zur Generierung und zum Umgang mit hinreichend starken Passwörtern hinzuweisen.

2) System-Anbieter von schulischen Informationssystemen, die eine Log-out-Funktion haben, haben System-Nutzer in einfacher und verständlicher Sprache auf die Wichtigkeit der Abmeldung vom schulischen Informationssystem nach Beendigung der Nutzung (Log-out) hinzuweisen.

3) System-Anbieter von schulischen Informationssystemen, die von privaten Endgeräten aus genutzt werden können, haben sicherzustellen, dass den System-Nutzern mindestens bei erstmaliger Nutzung die Information angezeigt wird, dass die Nutzung auf privaten Endgeräten ggf. unzulässig oder erlaubnisbedürftig ist oder bestimmten anderweitigen Anforderungen unterliegt.

Erläuterung

Der ordnungsgemäße Umgang mit Passwörtern ist ein wichtiger Baustein für die Erfüllung der Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) im Rahmen der Datensicherheit nach Art. 32 DS-GVO. Wenn in der Schule mit mobilen Geräten oder stationären Computern gearbeitet wird, ist es für die Gewährleistung der Vertraulichkeit zudem wichtig, dass sich die System-Nutzer (also vor allem die Schülerinnen und Schüler) nach der Nutzung abmelden (Log-out). Auf diese Weise wird verhindert, dass nachfolgende Nutzer (insbesondere andere Schülerinnen und Schüler) Zugriff auf personenbezogene Daten des vorhergehenden Nutzers haben.

Ein in der Praxis relevantes Problem ist die Speicherung personenbezogener Daten von Schülerinnen und Schülern auf privaten Endgeräten der Lehrkräfte. Auch hat der Einsatz privater Endgeräte durch die Schülerinnen und Schüler eine gewisse Verbreitung gefunden. Um den damit verbundenen Gefahren entgegenzutreten, hat der System-Anbieter darauf hinzuweisen, dass die Nutzung ggf. unzulässig oder erlaubnisbedürftig ist oder bestimmten anderweitigen Anforderungen unterliegt.

Umsetzungshinweis

Die Informationen zu den Passwörtern und zum Log-out können z. B. als elektronischer Flyer zum Download bereitgestellt werden. Alternativ kann z. B. ein System-Hinweis im schulischen Informationssystem angezeigt werden.

Die Stärke der von den System-Nutzern gewählten Passwörter sollte angezeigt werden, um eine sichere Passwortvergabe zu unterstützen. Die Nutzung eines Passwort-Managers kann empfohlen werden.

Die Informationen zur Nutzung privater Endgeräte können z. B. durch einen System-Hinweis nach dem erstmaligen Einloggen im schulischen Informationssystem erfolgen.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung

Landesgesetzliche Regelungen

In den Schulgesetzen der Länder finden sich Vorgaben zur Verarbeitung personenbezogener Daten auf privaten Endgeräten der Lehrkräfte. So muss die Verwendung der privaten Endgeräte in manchen Bundesländern durch die Schulleitung genehmigt werden, während andere Bundesländer eigene Löschfristen für personenbezogene Daten auf den privaten Endgeräten der Lehrkräfte vorsehen:

- Baden-Württemberg: Ziffer 1.13 VwV-Datenschutz an öffentlichen Schulen BW; Anlage 1 VwV-Datenschutz an öffentlichen Schulen BW.
- Bayern: Nr. 3.2.4 VollzBek DS Bay.
- Berlin: § 17 SchulDatenV Berlin; § 5 Abs. 4 DigLLV Berlin.
- Brandenburg: § 65 Abs. 5 BbgSchulG i.V.m. § 4 Abs. 1, § 5 DSV-BBG; Anlage 7 DSV-BBG.
- Bremen: § 4 Abs. 2 BremSchulDSG.
- Hamburg: § 3 Abs. 4 SchulDSV HA, sowie Richtlinie zur Verwendung privater Datenverarbeitungsgeräte (z. B. Personalcomputer) für dienstliche Verarbeitung personenbezogener Daten durch Lehrkräfte außerhalb von Diensträumen.
- Hessen: § 20 SchDSV-HE i.V.m. Anlage 1 Teil A Nr. 6.
- Mecklenburg-Vorpommern: § 7; Anlage 2 SchulDSVO M-V.
- Niedersachsen: S. Runderlass „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften“.
- Nordrhein-Westfalen: § 2 Abs. 2 i.V.m. Anlage 3 VO-DV I NRW (Datensatz bei Genehmigung der Verarbeitung personenbezogener Schülerinnen- und Schülerdaten auf privaten digitalen Geräten); RdErl. d. Ministeriums für Schule und Bildung, Nr. 11.1 „Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule“.
- Rheinland-Pfalz: Rheinland-Pfalz: § 89 Abs. 4 SchulO-RLP 2009, § 49 Abs. 4 Grund-SchulO 2008, § 55 Abs. 3 BBSSchulO.
- Saarland: § 17 SchulwDSV SL.
- Sachsen: Ziffer V Nr. 1-6 VwV Schuldatenschutz Sachsen.
- Sachsen-Anhalt: Runderlass „Verarbeitung personenbezogener Daten auf privaten Rechnern von Lehrkräften“.
- Schleswig-Holstein: § 30 Abs. 2 SchulG SH i.V.m. § 14 SchulDSVO SH.
- Thüringen: § 57 Abs. 8 Nr. 5 ThürSchulG i.V.m. § 136 Abs. 6 ThürSchulO und § 47 Abs. 7 ThürASObbS (Verwendung anderer als vom Schulträger zur Verfügung gestellter Datenverarbeitungsgeräte).

Nr. 3.7 - Übermittlung von Daten und Transportverschlüsselung
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Dies bedingt insbesondere einen hinreichenden Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen der Daten sowie vor bekannten Angriffsszenarien.
2) Der System-Anbieter setzt bei der Übermittlung personenbezogener Daten eine Transportverschlüsselung nach dem Stand der Technik ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Er muss die Spezifikationen dokumentieren, die er zur Festlegung seiner TOM in Bezug auf die Transportverschlüsselung nutzt. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen werden können. Bei verschlüsselter Übertragung sind die Schlüssel gemäß dem Stand der Technik sicher aufzubewahren. Der Zugriff zum Schlüssel muss kontrolliert werden.
3) Datenträger werden beim Transport vor dem Zugriff Unbefugter hinreichend sicher geschützt.

4) Der System-Anbieter protokolliert die Übermittlung personenbezogener Daten sowie den Transport von Datenträgern und stellt durch TOM sicher, dass der Transportweg beim Transport von Datenträgern überprüfbar und nachvollziehbar ist. Dies gilt auch für den Transport von Datenträgern vom und an den System-Kunden oder vom und an den Subauftragsverarbeiter.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern zu schützen.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Auf den Technischen Report BSI TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“ in der jeweils aktuellen Fassung wird hingewiesen. Die Verwendung von SSL (einschließlich der Version 3.0) ist kein sicheres Verfahren.

Es sollte eine Ende-zu-Ende-Verschlüsselung erfolgen. Sofern dies wegen fehlender Verfügbarkeit nicht möglich ist, kann eine Transportverschlüsselung genutzt werden. Die für die betroffenen Personen weiterhin bestehenden Risiken sollten jedoch durch andere angemessene Abhilfemaßnahmen getroffen werden. Die Abhilfemaßnahmen können sich zudem auf die allgemeine Dienstsicherheit und die Sicherheit der weiteren Systeme des System-Anbieters beziehen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 43 „Protokollieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen G 0.19 Offenlegung schützenswerter Informationen
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen G 0.46 Integritätsverlust schützenswerter Informationen
- BSI, IT Grundschutz Kompendium, CON 9 Informationsaustausch
- BSI, IT Grundschutz Kompendium OPS. Betrieb für Dritte 3.2.A20 Verschlüsselte Datenübertragung und -speicherung
- BSI, TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Version: 2025-01
- ISO/IEC 27002:2022 Ziff. 5.14 Informationsübermittlung
- ISO/IEC 27002:2022 Ziff. 7.10 Speichermedien
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.7 Informationsübertragung
- ISO/IEC 27701:2025 Ziff. B.3.20 Speichermedien
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 3.8 – Nachvollziehbarkeit der Datenverarbeitung
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e, f und Abs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter protokolliert Eingaben, Veränderungen und Löschungen personenbezogener Daten, die bei der Nutzung des schulischen Informationssystems durch den System-Kunden oder System-Nutzer oder bei administrativen Maßnahmen des System-Anbieters erfolgen, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung hinreichend sicherzustellen.

2) Der System-Anbieter erstellt Richtlinien für die Protokollierung, in denen die Anforderungen und Vorgaben an die Protokollierung beschrieben werden.

3) Der System-Anbieter stellt sicher, dass die Protokolldaten nur Informationen enthalten, die absolut notwendig sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen.

4) Der System-Anbieter hat die Protokolldaten sicher aufzubewahren und vor Manipulationen zu schützen, was insbesondere einen hinreichenden Schutz gegen bekannte Angriffsszenarien und Maßnahmen zur Erkennung von Manipulationen umfasst. Er stellt sicher, dass auch Administratoren die eigenen Aktivitäten in den aufgezeichneten Protokolldaten nicht manipulieren können.

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um ggf. Zugriffsrechte für die Zukunft anders zu gestalten. Zur sicheren Aufbewahrung der Protokolldaten gehört auch, dass die Auswertbarkeit der Protokolldaten sichergestellt ist.

Da im Rahmen von Protokollierungen regelmäßig personenbezogene Daten anfallen, unterliegt der Umgang mit Protokollierungsdaten ebenfalls datenschutzrechtlichen Anforderungen. Dabei ist besonderes Augenmerk auf die Grundsätze der Datenminimierung und Zweckbindung aus Art. 5 Abs. 1 lit. c und b DS-GVO zu legen. Die Protokolldaten dürfen nur Informationen enthalten, die absolut notwendig sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen.

Umsetzungshinweis

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten sollten auf ausgewählte und autorisierte Mitarbeitende des System-Anbieters beschränkt werden und eine Multi-Faktor-Authentifizierung erfordern. Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware sollte unabhängig überwacht werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 43 „Protokollieren“
- BSI, IT Grundschutz Kompendium OPS.1.1.5 Protokollierung
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 3.9 - Pseudonymisierung
(Art. 32 Abs. 1 lit. a DS-GVO)

Kriterium

1) Der System-Anbieter ermöglicht es dem System-Kunden, pseudonymisierte Daten zu verarbeiten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.[28]

2) Eine De-Pseudonymisierung erfolgt nur auf dokumentierte Weisung des System-Kunden. Der System-Anbieter stellt sicher, dass die De-Pseudonymisierung dokumentiert wird.

3) Wird die Pseudonymisierung vom System-Anbieter durchgeführt, stellt dieser durch TOM sicher, dass die zusätzlichen Informationen zur Identifizierung der betroffenen Person gesondert aufbewahrt werden. Der Datensatz mit der Zuordnung des Kennzeichens zu einer Person muss so geschützt werden, dass zu erwartende Manipulationsversuche ausgeschlossen werden. Insbesondere ist der Kreis der Mitarbeitenden, die den Personenbezug herstellen und die Pseudonymisierung aufheben können, auf das unbedingt Erforderliche zu begrenzen.

4) Wird die Pseudonymisierung vom System-Anbieter durchgeführt, verfolgt er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend, mindestens jährlich, und stellt sicher, dass seine Verfahren dem Stand der Technik entsprechen.

Erläuterung

Das Kriterium verlangt nicht, dass der System-Anbieter von sich aus alle verarbeiteten Daten pseudonymisieren muss. Er muss aber – soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht – in der Lage sein, pseudonyme Daten zu verarbeiten.

Die Pseudonymisierung wird neben der Verschlüsselung in Art. 32 Abs. 1 lit. a DS-GVO explizit als einzusetzende Sicherheitsmaßnahme benannt. Eine Pseudonymisierung ist gemäß Art. 4 Nr. 5 DS-GVO die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Die Pseudonymisierung trägt dazu bei, die Gewährleistungsziele der Datenminimierung (SDM C1.1) und der Nichtverkettung (SDM C1.5) zu fördern. Da durch Pseudonymisierung Dritte selbst bei einem unbefugten Zugriff auf das schulische Informationssystem keine Kenntnis von den personenbezogenen Daten erlangen können oder die Herstellung des Personenbezugs zumindest erheblich erschwert wird, mindert die Pseudonymisierung die Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen. Welche Zwecke mit der Pseudonymisierung verfolgt werden, hängt von der konkreten Verarbeitungssituation und der Vereinbarung zwischen dem System-Kunden und dem System-Anbieter ab.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Der System-Anbieter sollte durch TOM sicherstellen, dass eine Pseudonymisierung der personenbezogenen Daten nicht aufgehoben werden kann (bspw. Sicherstellung, dass der Schlüssel des System-Kunden nicht bekannt ist).

Um eine weisungsgetreue De-Pseudonymisierung durchführen zu können, sollten mit dem System-Kunden dokumentierte Fälle von gewünschten Aufdeckungen definiert werden. Aus der Dokumentation der De-Pseudonymisierung sollte hervorgehen, wer die De-Pseudonymisierung durchgeführt hat. In ihr sollten jedoch keine Angaben enthalten sein, die Rückschlüsse auf die dem Pseudonym zugrunde liegenden Identitätsdaten erlauben.

[28] Das Kriterium verlangt nicht, dass der System-Anbieter von sich aus alle verarbeiteten Daten pseudonymisieren muss. Er muss aber – soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht – in der Lage sein, pseudonyme Daten zu verarbeiten.

Für die Überwachung des Pseudonymisierungsprozesses kann der System-Anbieter einen geeigneten Fachverantwortlichen bestimmen, der einen einheitlichen Einsatz bei der Pseudonymisierung koordiniert und die Verantwortung für wichtige Entscheidungen übernimmt.

Werden Pseudonyme durch Berechnungsverfahren erstellt, sollten diese dem Stand der Technik entsprechen (z. B. BSI TR-02102-1). Die getrennte Aufbewahrung des Datensatzes mit der Zuordnung des Kennzeichens zu einer Person bedarf eines dokumentierten Berechtigungskonzepts. Der Zugriff auf diesen Datensatz sollte auf ein absolutes Minimum an vertrauenswürdigen Personen eingeschränkt werden („Need-to-Know-Prinzip"). Jeder Zugriff auf den Datensatz mit der Zuordnungsinformation sollte nach dem Vier-Augen-Prinzip erfolgen. Sofern dies nicht möglich ist, sollte jeder Zugriff personenbezogen protokolliert werden.

Der System-Anbieter sollte öffentlich bekannt geben, welche technischen Standards sein Pseudonymisierungsverfahren erfüllt.

- EDSA, Guidelines 01/2025 on Pseudonymisation
- ISO/IEC 27002:2022 Ziff. 8.11 Datenmaskierung
- ISO/IEC 20889:2018 Informationstechnik-Sicherheitsverfahren-Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre

Nr. 3.10 - Anonymisierung
(Art. 5 Abs. 1 lit. c DS-GVO)

Kriterium

1) Der System-Anbieter ermöglicht es dem System-Kunden, anonyme bzw. anonymisierte Daten zu verarbeiten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.[29]

2) Wird die Anonymisierung vom System-Anbieter durchgeführt, verfolgt er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend und stellt sicher, dass seine Verfahren dem Stand der Technik entsprechen.

Erläuterung

Das Kriterium verlangt nicht, dass der System-Anbieter von sich aus alle verarbeiteten Daten anonymisieren muss. Er muss aber – soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht – in der Lage sein, anonyme Daten zu verarbeiten.

Die Anonymisierung ist neben dem Verzicht der Datenerhebung die wirksamste Maßnahme zur Datenvermeidung und Datenminimierung. Sie trägt dazu bei, das Gewährleistungsziel der Datenminimierung (SDM C1.1) zu fördern.

Die DS-GVO selbst definiert die Anonymisierung nicht. Nach EG 26 Satz 5 DS-GVO gilt die DS-GVO nicht für „anonyme Informationen […], d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann". Daten sind somit anonym i.d.S., wenn sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, wenn sie also nicht personenbezogen sind.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Die Anonymisierungsverfahren sollten den besonderen Anforderungen der Datenverarbeitung im Kontext der Schule Rechnung tragen.

Technische Schutzmaßnahmen zur Wahrung der Anonymisierung können z. B. die Verhinderung von automatischer Datenaggregation und -synthese umfassen, die zur Rückgängigmachung der Anonymisierung führen könnten, sowie die Verwaltung der Zugriffsrechte der autorisierten Mitarbeitenden, um böswilliges Verhalten zu verhindern. Organisatorische Schutzmaßnahmen stellen

[29] Das Kriterium verlangt nicht, dass der System-Anbieter von sich aus alle verarbeiteten Daten anonymisieren muss. Er muss aber – soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht – in der Lage sein, anonyme Daten zu verarbeiten.

u.a. sicher, dass Mitarbeitende kein Verhalten an den Tag legen, das auf die Rückgängigmachung der Anonymisierung abzielt, wie z. B. das Ausfragen von System-Kunden über ihre Anonymisierungspraktiken, um potenzielle Schwachstellen oder Schwachpunkte der angewandten Anonymisierungstechniken auszunutzen.

Der System-Anbieter sollte öffentlich bekannt geben, welche technischen Standards sein Anonymisierungsverfahren erfüllt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2022 Ziff. 8.11 Datenmaskierung
- ISO/IEC 20889:2018 Informationstechnik-Sicherheitsverfahren-Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre

Nr. 3.11 – Verschlüsselung verarbeiteter Daten
(Art. 32 Abs. 1 lit. a DS-GVO, Art. 5 Abs. 1 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter ermöglicht dem System-Kunden die Verarbeitung von verschlüsselten Daten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.

2) Wird die Verschlüsselung vom System-Anbieter durchgeführt, verhindert er durch TOM den unbefugten Zugriff auf Schlüssel. Der Kreis der Mitarbeitenden, die die Verschlüsselung aufheben können, ist auf das unbedingt Erforderliche zu begrenzen.

3) Wird die Verschlüsselung vom System-Anbieter durchgeführt, verfolgt er laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen, insbesondere ein sicheres Schlüsselmanagement, entsprechen dem Stand der Technik. Er prüft regelmäßig die Eignung seiner Verschlüsselungsverfahren und aktualisiert diese bei Bedarf. Die Prüfung ist zu dokumentieren.

4) Erfolgt die Verschlüsselung durch den System-Kunden, unterstützt der System-Anbieter, soweit dies in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung vereinbart ist, den System-Kunden auf dessen Weisung hin bei der Verschlüsselung und Entschlüsselung der Daten. Die Unterstützung erfolgt mindestens in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung. Der System-Anbieter stellt sicher, dass seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung dem Stand der Technik entsprechen.

Erläuterung

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DS-GVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM C1.4 und C1.3) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, so dass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Soweit der System-Anbieter Daten verschlüsselt, sollte die Schlüsselerzeugung in einer sicheren Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptografische Schlüssel sollten möglichst nur einem Einsatzzweck dienen und generell nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Die Speicherung sollte stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels auszuschließen. Schlüsselwechsel sollten regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern. Administratoren des System-Anbieters sollten keinen Zugriff auf die Schlüssel des System-Kunden oder auf Schlüssel der System-Nutzer (sofern diese vorhanden sein sollten) haben.

Um unbefugte Zugriffe auf den Schlüssel hinreichend sicher auszuschließen, sollte der System-Anbieter sicherstellen, dass Zugriffe auf Schlüssel umfassend überwacht und geschützt werden.

Auf den Technischen Report BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, in der jeweils aktuellen Fassung wird hingewiesen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 11 „Aufbewahren“
- BSI, IT-Grundschutz CON.1 Kryptokonzept
- ISO/IEC 11770 Informationstechnik - Sicherheitsverfahren - Schlüsselmanagement Teil 1-7
- ISO/IEC 27002:2022 Ziff. 8.24 Verwendung von Kryptographie
- ISO/IEC 27701:2025 Ziff. B.3.26 Verwendung von Kryptographie

Nr. 3.12 - Getrennte Verarbeitung
(Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter verarbeitet die Daten des System-Kunden logisch oder physisch getrennt von den Datenbeständen anderer System-Kunden und von anderen Datenbeständen des System-Anbieters und ermöglicht dem System-Kunden, die Datenverarbeitung nach Verarbeitungszwecken zu trennen.

2) Der System-Anbieter sieht TOM vor, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, um eine Verletzung der Datentrennung zu verhindern, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter sowie vor bekannten Angriffsszenarien gegen das Trennungsgebot einschließt. Der System-Anbieter kann Verstöße gegen das Trennungsgebot nachträglich feststellen.

Erläuterung

Das Kriterium fördert die Gewährleistungsziele der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM C1.2 – C1.5) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DS-GVO ab. Eine sichere Mandantentrennung schützt die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung und verhindert eine unerwünschte Verkettung der Daten.

Umsetzungshinweis

Daten sollten auf gemeinsam genutzten virtuellen und physischen Ressourcen (Speichernetz, Arbeitsspeicher) gemäß einem dokumentierten Konzept sicher und strikt separiert werden.

Der System-Anbieter sollte technische und organisatorische Überwachungsverfahren und -systeme betreiben, um Angriffe (bspw. Cross-VM Attacks) und böswilliges Verhalten feststellen und unterbinden zu können.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe Mandantenfähigkeit
- SDM-Baustein 50 „Trennen“
- BSI, IT Grundschutz Kompendium SYS 1 Server, SYS 2 Desktop Systeme
- ISO/IEC 27002:2022 Ziff. 8.22 Trennung von Netzwerken

Nr. 3.13 – Wiederherstellbarkeit nach einem Zwischenfall
(Art. 32 Abs. 1 lit. c DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass die Verfügbarkeit der verarbeiteten personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann und der Zwischenfall nicht zu einem endgültigen Datenverlust führt.

2) Werden besonders relevante Daten über den schulischen Werdegang der Schülerinnen und Schüler ausschließlich beim System-Anbieter verarbeitet, insbesondere die Stammblätter der Schülerinnen und Schüler, Zeugnisse, Prüfungsunterlagen und Abschriften der Abschlusszeugnisse, sichert sich der System-Anbieter auch gegen außergewöhnliche Zwischenfälle so zuverlässig ab, dass diese Zwischenfälle nicht zu einem endgültigen Datenverlust führen.

3) Der System-Anbieter erstellt ein Datensicherungskonzept, das insbesondere ein risikoabhängiges, regelmäßiges Erstellen von Sicherungskopien der personenbezogenen Daten vorsieht.

4) Besonders relevante Daten i.S.v. Abs. 2 sind im Falle eines Zwischenfalls i.S.v. Abs. 1 für den System-Kunden in einem Format abrufbar, das die Speicherung in einer nicht-digitalen Form ermöglicht.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit (SDM C1.2) und adressiert Zwischenfälle (engl.: „incident"), die zu einer Einschränkung der Verfügbarkeit der personenbezogenen Daten oder des Zugangs zu ihnen führen.

Physischen Zwischenfälle können z. B. den Verlust von Speichermedien oder die Beschädigung bzw. Zerstörung von Geräten oder Räumen, die mit der Verarbeitung in Zusammenhang stehen, umfassen. Zu technischen Zwischenfällen zählen z. B. Löschbefehle nach Umgehen von Zugangskontrollmechanismen oder Ransomware-Angriffe.[30]

Gemäß Art. 32 Abs. 1 lit. c DS-GVO soll die Wiederherstellung „rasch" (engl.: „in a timely manner") erfolgen. Was als „rasch" gilt, hängt auch von der Schwere des Zwischenfalls und der Bedeutung der Systeme und Daten ab. Z. B. sind an die Wiederherstellbarkeit der Daten in Systemen, die für fristgebundene Aktivitäten (z. B. Abiturprüfungen) benötigt werden, insoweit strengere Anforderungen zu stellen als an die Wiederherstellung von Daten in einem Datenarchiv.

Werden besonders relevante Daten über den schulischen Werdegang der Schülerinnen und Schüler beim System-Anbieter gespeichert, gewährleistet dieser für sein System einen hohen Schutz, der außergewöhnliche, aber theoretisch nicht auszuschließende Zwischenfälle so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu einem endgültigen Datenverlust führen. Zwischenfälle sind außergewöhnlich, aber theoretisch nicht auszuschließen, wenn sie nicht vorkommen sollen und nach der Lebenserfahrung nicht auftreten, aber gleichwohl in extrem seltenen Einzelfällen zu beobachten sind, wie etwa „Black Swan"-Ereignisse oder ein unkontrollierbarer Blitzeinschlag ins Rechenzentrum. Diese Anforderung wird allerdings nur dann ausgelöst, wenn diese besonders relevanten Daten ausschließlich beim System-Anbieter verarbeitet werden.

Umsetzungshinweis

Zur Wiederherstellung von Daten sollte ein System-Anbieter ein wirksames Datensicherungskonzept erstellen, in dem er Systeme zu Datensicherungen, Pläne zur Wiederherstellung und zur Schadensbegrenzung sowie einen Plan zur regelmäßigen Überprüfung und Aktualisierung der vorgesehenen Maßnahmen vorsieht.

[30] Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Art. 32 DS-GVO Rn. 54.

Es sollten regelmäßig Sicherheitskopien von Daten, Konfigurationen, Datenstrukturen etc. gemäß einem Datensicherungskonzept angefertigt werden. Die Wiederherstellbarkeit der Sicherheitskopien sollte regelmäßig überprüft werden.

Die Datensicherungsstrategien und -maßnahmen des Datensicherungskonzepts sollten für System-Kunden transparent definiert werden, so dass alle Informationen nachvollziehbar sind, einschließlich Umfang, Speicherintervallen, Speicherzeitpunkten und Speicherdauern.

Neben der Erstellung von Sicherheitskopien sollte der System-Anbieter ein Notfallmanagement mit entsprechenden Notfallplänen etablieren.

Die Maßnahmen für die Sicherung der besonders relevanten Daten i.S.d. Abs. 2 sollten darüber hinaus beinhalten:

- Die Datensicherungen sollten an einem oder mehreren externen Orten in ausreichender Entfernung redundant aufbewahrt werden, um vor Schäden am Hauptstandort geschützt zu sein (s. ISO/IEC 27002 Ziff. 12.3.1). Datensicherungen sollten mittels Verschlüsselung auf dem aktuellen Stand der Technik geschützt werden (zum Begriff des Standes der Technik s. das Glossar).
- Der Zugriff auf die gesicherten Daten ist auf autorisiertes Personal beschränkt. Wiederherstellungsprozesse beinhalten Kontrollmechanismen, die sicherstellen, dass Wiederherstellungen ausschließlich nach Genehmigung durch hierfür autorisierte Personen gemäß den vertraglichen Vereinbarungen mit dem System-Kunden oder den internen Richtlinien des System-Anbieters erfolgen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM, Abschnitt B1.20 Wiederherstellbarkeit
- BSI, IT Grundschutz Kompendium OPS Betrieb
- BSI, IT Grundschutz Kompendium DER Detektion und Reaktion
- BSI, IT Grundschutz Kompendium SYS 1 Server, SYS 2 Desktop Systeme
- ISO/IEC 27002:2022 Ziff. 5.30 IKT-Bereitschaft für Business-Continuity
- ISO/IEC 27002:2022 Ziff. 8.13 Sicherung von Informationen
- ISO/IEC 27701:2025 Ziff. B.3.26 Sicherung von Informationen

Nr. 4 – Sicherstellung der Weisungsbefolgung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, Art. 29, Art. 32 Abs. 4 DS-GVO)

Kriterium

Der System-Anbieter verfügt über einen Prozess, damit die Datenverarbeitung im Auftrag – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – durch den System-Anbieter sowie ihm unterstellte Personen ausschließlich auf dokumentierte Weisung des System-Kunden erfolgt (s. Nr. 1.4), sofern der System-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist. Für einen solchen Fall stellt der Prozess zudem sicher, dass der System-Anbieter dem System-Kunden diese rechtlichen Anforderungen vor der Verarbeitung mitteilt, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Erläuterung

Der Auftragsverarbeiter (hier der System-Anbieter) darf personenbezogene Daten grundsätzlich nur auf Weisung des Verantwortlichen (hier des System-Kunden) verarbeiten (s. die Erläuterungen zu Nr. 1.4). Gemäß der „Gefolgschaftspflicht“[31] in Art. 29 DS-GVO dürfen der System-Anbieter und

[31] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 29 DS-GVO Rn. 1.

ihm unterstellte Personen, die Zugang zu personenbezogenen Daten haben, die Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten.

Der System-Anbieter verarbeitet personenbezogene Daten ohne Weisung, sofern er durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und Art. 29 DS-GVO). Beispiele hierfür sind Übermittlungen des System-Anbieters an Ermittlungsbehörden in Strafsachen, Steuerangelegenheiten oder staatsschutz- und geheimdienstrelevante Sachverhalte.

Umsetzungshinweis

Der System-Anbieter sollte die Weisungsbefolgung auch in einer etwaigen Datenverarbeitungskette sicherstellen, indem er entsprechende Garantien nachgelagerter Auftragsverarbeiter einholt. Darüber hinaus sollte der System-Anbieter regelmäßig kontrollieren, ob die Weisungen des System-Kunden eingehalten werden.

Da die Weisungsbefolgung essenziell für die Auftragsverarbeitung ist, sollte der System-Anbieter diese gegen technische und organisatorische Fehler und Manipulationsversuche bei der Erteilung von Weisungen absichern. Maßnahmen der Datensicherheit wie bspw. die Zugangs- und Zugriffskontrolle (Nr. 3.4 und Nr. 3.5) und die Gewährleistung der Nachvollziehbarkeit der Datenverarbeitung (Nr. 3.8) tragen zur Sicherstellung der Weisungsbefolgung bei, so dass die hierzu angegebenen Umsetzungshinweise ebenfalls berücksichtigt werden sollten.

Meistens werden Weisungen mittels Softwarebefehlen erteilt oder automatisiert ausgeführt (z. B. durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe). Weisungen können aber auch per Telefon, E-Mail, Fax oder ein Ticket-System erteilt werden. Dabei ist sicherzustellen, dass die Anweisung von einer berechtigten Person kommt.

Im besonderen Kontext der schulischen Informationssysteme, insbesondere in Form von Online-Lernplattformen, werden die Verarbeitungsvorgängen vor dem Einsatz eines solchen Systems festgelegt. Dies kann im Rahmen einer Nutzer- und Nutzungsordnung geschehen,[32] die die Schule als verantwortliche Stelle und System-Kunde festlegt und die der System-Anbieter zu befolgen hat. Eine solche Nutzer- und Nutzungsordnung ist als Weisung i.S.d. Art. 28 DS-GVO zu verstehen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- Klausel 7.1 im Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- DSK, Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 27701:2025 Ziff. B.2.2.3 Ziele der Organisation
- ISO/IEC 27701:2025 Ziff. B.2.2.5 Verstoßende Anweisungen
- ISO/IEC 27701:2025 Ziff. B.2.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten

Nr. 5 – Hinweis- und Mitwirkungspflicht bei datenschutzwidrigen Weisungen

Erläuterung

[32] DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 10.

Die Schulen und Schulträger als System-Kunden sind im Bereich des Datenschutzes regelmäßig auf Unterstützung durch die System-Anbieter angewiesen, da die System-Anbieter häufig einen besseren Einblick in die relevanten Verarbeitungsvorgänge sowie unmittelbaren Zugriff auf die benötigten technischen Einrichtungen haben. Den Schulen fehlen ggf. auch die Kapazitäten, sich mit Fragen des Datenschutzes bei Nutzung schulischer Informationssysteme vertieft auseinanderzusetzen. Zudem wird es sich dabei des Öfteren um Fragen handeln, die beim System-Anbieter wiederholt auftreten und von ihm zentral für zahlreiche Fälle geklärt werden können.

In rechtlicher Hinsicht bestimmt Art. 28 Abs. 3 UAbs. 2 DS-GVO, dass der Auftragsverarbeiter (also der System-Anbieter) den Verantwortlichen (also den System-Kunden) unverzüglich informiert, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Dies setzt voraus, dass der System-Anbieter über hinreichend und fortlaufend geschulte Mitarbeitende verfügt (Nr. 2.6), die in der Lage sind, rechtswidrige Weisungen zu erkennen. Den System-Anbieter treffen mithin Mitwirkungspflichten, um den System-Kunden bei der Wahrnehmung seiner datenschutzrechtlichen Pflichten, die ihn als Verantwortlichen treffen, zu unterstützen. Den System-Anbieter trifft indes keine Pflicht, die Weisungen des System-Kunden sowie die Verarbeitungsvorgänge einer systematischen und detaillierten Prüfung zu unterwerfen. Eine Delegation der datenschutzrechtlichen Pflichten des verantwortlichen System-Kunden auf den System-Anbieter bzw. eine Verantwortungsübertragung findet nicht statt.

Nr. 5.1 – Hinweispflicht bei datenschutzwidrigen Weisungen
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m. Art. 29 DS-GVO)

Kriterium

1) Der System-Anbieter informiert den System-Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung gegen datenschutzrechtliche Vorschriften verstößt. Er implementiert einen entsprechenden Prozess, damit der System-Kunde in derartigen Fällen unverzüglich informiert wird.

2) Der System-Anbieter implementiert einen Prozess, der sicherstellt, dass seine Mitarbeitenden Weisungen des System-Kunden sowie darauf beruhende Datenverarbeitungen, die offensichtlich gegen datenschutzrechtliche Vorschriften verstoßen, erkennen können. Dieser Prozess verlangt zumindest, dass die Mitarbeitenden hinreichend und fortlaufend im Bereich Datenschutz und Datensicherheit geschult werden und dass sie in Zweifelsfällen den Datenschutzbeauftragten (sofern ein solcher benannt wurde) und die zuständigen Aufsichtsbehörden kontaktieren und um Rat fragen.

Erläuterung

Die Verantwortung für die Übereinstimmung einer Weisung mit dem geltenden Datenschutzrecht liegt beim System-Kunden als dem Verantwortlichen. Dennoch darf der System-Anbieter eine Weisung, deren Übereinstimmung mit dem Datenschutzrecht er bezweifelt, nicht unbesehen ausführen. Vielmehr hat er den System-Kunden gemäß Art. 28 Abs. 3 UAbs. 2 DS-GVO zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt (s. Nr. 1.4), und die Entscheidung des System-Kunden abwarten. Der System-Anbieter hat den System-Kunden unverzüglich, also ohne schuldhaftes Zögern, zu informieren.

Zu den maßgeblichen datenschutzrechtlichen Vorschriften zählen neben der DS-GVO auch andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten. Letzteres schließt die datenschutzrechtlichen Vorschriften von Bund und Ländern mit ein. Im Kontext schulischer Informationssysteme sind daher auch die datenschutzrechtlichen Vorgaben in den schuldatenschutzrechtlichen Vorschriften der Länder von Bedeutung.

Ein offensichtlicher Verstoß gegen datenschutzrechtliche Vorschriften liegt vor, wenn sich der Verstoß bei verständiger Würdigung aller in Betracht kommenden Umstände einem geschulten Mitarbeitenden (s. Nr. 2.6) aufdrängen muss, wenn er also „für einen unvoreingenommenen, mit den in Betracht kommenden Umständen vertrauten, verständigen Beobachter ohne weiteres ersichtlich ist“.[33]

[33] BVerwG, NVwZ 1987, 230 (230) zu § 44 VwVfG.

Den System-Anbieter trifft keine Pflicht, die Weisungen des System-Kunden sowie die Verarbeitungsvorgänge einer systematischen und detaillierten Prüfung zu unterwerfen.[34] Eine Delegation der datenschutzrechtlichen Pflichten des verantwortlichen System-Kunden auf den System-Anbieter bzw. eine Verantwortungsübertragung findet nicht statt.

Umsetzungshinweis

Bei der Aufnahme von Weisungen in die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung und bei jeder abgegebenen Weisung sollte der System-Anbieter seinen Datenschutzbeauftragten (sofern ein solcher benannt wurde) konsultieren, wenn sich die Datenschutzwidrigkeit der Weisung einem datenschutzrechtlich geschulten Mitarbeitenden des schulischen Informationssystems aufdrängt.

Bei Massengeschäften, in denen der System-Kunde durch die Auswahl des schulischen Informationssystems aufgrund einer Systembeschreibung des System-Anbieters die Weisung erteilt, sollte der System-Anbieter TOM vorsehen, die den System-Kunden darauf hinweisen, wenn er das System datenschutzwidrig entgegen der Systembeschreibung nutzt. Dazu zählt bspw. ein Informationstext, der den System-Kunden warnt, wenn die vom System-Anbieter zur Verfügung gestellten Datensicherungsmaßnahmen wie Verschlüsselung und Pseudonymisierung nicht genutzt bzw. deaktiviert werden.

Der System-Anbieter sollte organisatorische Prozesse spezifizieren und dokumentieren, welche die Ansprechpartner, deren Verantwortlichkeiten, Vorgehensweisen und Meldewege im Falle einer Feststellung einer datenschutzwidrigen Weisung regeln. Diese Prozesse können bspw. in bestehende Incident- und Troubleshooting-Management-Prozesse verankert werden.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2025 Ziff. B.2.2.5 Verstoßende Anweisungen

Nr. 5.2 – Rechtmäßigkeit der Datenverarbeitung
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m. Art. 29 DS-GVO)

Kriterium

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung
    a. offensichtlich unrechtmäßig ist,
    b. dem vertraglich vereinbarten Zweck, zu dem das schulische Informationssystem eingesetzt werden soll, offensichtlich zuwiderläuft,
    c. zu dem vereinbarten Zweck offensichtlich nicht erforderlich ist und
    d. Daten betrifft, die offensichtlich nicht verarbeitet werden dürfen.
2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

Erläuterung

Die Pflicht in Nr. 5.2 steht unter dem Vorbehalt des Möglichen. Es bedeutet, dass dem System-Anbieter nichts in technischer oder rechtlicher Hinsicht Unmögliches abverlangt werden darf. Der System-Anbieter hat nur auf Verarbeitungsvorgänge zu achten, die in seiner Sphäre erfolgen. Es ist nicht Aufgabe des System-Anbieters, die Weisungen des System-Kunden sowie die Verarbeitungsvorgänge einer systematischen und detaillierten Prüfung zu unterwerfen. Der System-Anbieter hat aber auf offensichtliche Verstöße zu achten und darf diese nicht einfach ignorieren. Eine Übertragung der datenschutzrechtlichen Verantwortlichkeit i.S.v. Art. 4 Nr. 7 DS-GVO vom System-Kunden auf den System-Anbieter ist damit nicht verbunden.

Die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler ist rechtmäßig, wenn sie auf eine Rechtsgrundlage gestützt werden kann (Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 DS-GVO).

[34] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 83.

Als Rechtsgrundlage im Rahmen des Lehr- und Lernbetriebs kommt zunächst eine Einwilligung in Betracht (vgl. Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 4 Nr. 11, Art. 7 und 8 DS-GVO), bei der aufgrund des im Bildungs- und Erziehungswesen bestehenden Subordinations- und Näheverhältnisses zwischen Schülerinnen und Schülern und Lehrkräften sowie den Schulen, Schulbehörden und Schulträgern die Freiwilligkeit in Frage steht. Soweit die Einbindung eines schulischen Informationssystems in den Unterricht bedingt, dass dieses von allen Schülerinnen und Schüler genutzt wird, wäre es zudem problematisch, wenn einzelne Schülerinnen und Schüler (bzw. deren Erziehungsberechtigte) eine Einwilligung verweigern oder eine bereits erteilte Einwilligung widerrufen (Art. 7 Abs. 3 DS-GVO). In Einzelfällen kann eine Einwilligung trotzdem rechtlich zulässig sein (wenn z. B. im berufsschulischen Bereich die Mitarbeitenden eines Ausbildungsbetriebs ein schulisches Informationssystem nutzen wollen und dafür ein entsprechender Zugang eingerichtet werden muss). Als Standard-Rechtsgrundlage für die Verarbeitung der Daten von zahlreichen Schülerinnen und Schülern im Lernalltag einer Schule taugt die Einwilligung indes nicht als Rechtsgrundlage.

Auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO kann die Datenverarbeitung aufgrund von Art. 6 Abs. 1 UAbs. 2 DS-GVO nicht gestützt werden. Die Rechtsgrundlage für die Datenverarbeitung wird sich daher regelmäßig aus Art. 6 Abs. 1 UAbs. 1 lit. e und Abs. 3 DS-GVO i.V.m. dem nationalen Recht ergeben. Dabei ist auf das jeweilige nationale Schulrecht (in Deutschland: das Schulrecht der Bundesländer) abzustellen.

Die Schulgesetze bzw. schuldatenschutzrechtlichen Vorschriften der Länder können als Parlamentsgesetze oder Rechtsverordnungen eine Rechtsgrundlage für die Verarbeitung gemäß Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO sein. Erlasse und Verwaltungsvorschriften fallen als interne Dienstanweisungen ohne unmittelbare Außenwirkung nicht hierunter. Daher ist z. B. die Verwaltungsvorschrift des Kultusministeriums Baden-Württemberg über den Datenschutz an öffentlichen Schulen vom 4. Juli 2019[35] keine nationale Rechtsgrundlage i.S.d. DS-GVO. Zur besseren Orientierung werden die einschlägigen Verwaltungsvorschriften bei den einzelnen Kriterien zusammen mit den maßgeblichen Landesschulgesetzen aufgeführt. Der Anwender des Kataloges hat dabei aber zu beachten, dass es ggf. einer Rechtsgrundlage mangelt.

Die Pflicht, die jeweilige Verarbeitung personenbezogener Daten auf eine Rechtsgrundlage zu stützen und rechtmäßig durchzuführen, trifft den Verantwortlichen, also den System-Kunden. Die Schulen (etc.) als System-Kunden sind dabei aber ggf. auf Unterstützung durch den jeweiligen System-Anbieter angewiesen, da dieser häufig einen besseren Einblick in die relevanten Verarbeitungsvorgänge sowie unmittelbaren Zugriff auf die benötigten technischen Einrichtungen hat. Den Schulen fehlen ggf. auch die Kapazitäten, sich mit Fragen des Datenschutzes bei Implementierung schulischer Informationssysteme vertieft auseinanderzusetzen.

In rechtlicher Hinsicht bestimmt Art. 28 Abs. 3 UAbs. 2 DS-GVO, dass der Auftragsverarbeiter (also der System-Anbieter) den Verantwortlichen (also den System-Kunden) unverzüglich informiert, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Das kann der System-Anbieter aber nur, wenn er bei Weisungen des System-Kunden auf offensichtliche Rechtsverstöße achtet.

Landesgesetzliche Regelungen

Rechtsgrundlagen für eine rechtmäßige Verarbeitung der personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften und anderweitigen Angestellten sowie Erziehungsberechtigten finden sich insbesondere in den folgenden in landesrechtlichen Vorschriften. Soweit in einzelnen Ländern keine spezifischen schuldatenschutzrechtlichen Vorschriften bestehen, gelten die allgemeinen datenschutzrechtlichen Vorschriften (insbesondere die DS-GVO und die ergänzenden allgemeinen Landesdatenschutzgesetze).

- Baden-Württemberg: § 115 Abs. 3a, Abs. 4 SchulG BW (der auf das LDSG-BW verweist); § 115b SchG BW zum Einsatz digitaler Medien im Unterricht; VwV-Datenschutz an öffentlichen Schulen BW.
- Bayern: Art. 85 Abs. 1, Abs. 2 BayEUG und Art. 85a Abs. 2 BayEUG, beide i.V.m. § 46 BaySchO und Anlage 2 BaySchO.
- Berlin: § 64 SchulG-BE, insbesondere § 64 Abs. 1 SchulG-BE sowie § 64a SchulG-BE (sofern System-Anbieter an der Datenverarbeitung des Fachverfahrens mitwirken); außerdem

[35] Verwaltungsvorschrift des Kultusministeriums Baden-Württemberg über den Datenschutz an öffentlichen Schulen vom 4. Juli 2019, Az.: 13-0557.0/106.

§§ 1-4 SchulDatenV und DigLLV Berlin zur Konkretisierung der Verarbeitungsbefugnisse der §§ 64 ff. SchulG-BE.

- Brandenburg: §§ 65 Abs. 1 bis Abs. 4, Abs. 10 BbgSchulG; zu den erlaubten Datenarten vgl. außerdem: § 1 i.V.m. Anlage 1 bis 9 und zur Erforderlichkeit § 2 DSV-BBG.
- Bremen: § 2 Abs. 1 i.V.m. § 4 Abs. 1 BremSchulDSG i.V.m. SchDVVO Bremen.
- Hamburg: § 98 HmbSG, insbesondere § 98 Abs. 1 HmbSG; § 101 HmbSG i.V.m. § 1 SchulDSV HA; außerdem: § 3 HmbSfTG.
- Hessen: §§ 83, 83a SchulG-HE, insbesondere § 83 Abs. 1 SchulG-HE i.V.m. § 2 SchDSV-HE i.V.m. Anlage 1, 2 SchDSV-HE.
- Mecklenburg-Vorpommern: § 70 SchulG M-V i.V.m. § 1 Abs. 1 i.V.m. Anlage 1 SchulDSVO M-V (erlaubte Datenarten); § 5a Abs. 7 SchulDSVO M-V zu Kategorien personenbezogener Daten, die in einer Lernsoftware verarbeitet werden dürfen.
- Niedersachsen: § 31 NSchulG (Verarbeitung personenbezogener Daten), insbesondere § 31 Abs. 1 NSchulG (Verarbeitung).
- Nordrhein-Westfalen: § 120 SchulG NRW (Schutz der Daten von Schülerinnen und Schülern und Eltern), insbesondere Abs. 1 (Verarbeitung), Abs. 2 (Datenabgabe und Einwilligung), Abs. 5 (Einsatz digitaler Lehr- und Lernmittel, Lehr- und Lernsysteme und Arbeits- und Kommunikationsplattformen einschließlich Videokonferenzsysteme), § 121 SchulG NRW (Schutz der Daten des Personals im Schulbereich); außerdem VO-DV I NRW (Daten von Schülerinnen und Schülern sowie Eltern) und VO-DV II NRW (Lehrkräfte sowie sonstige Personen im Schulbereich); Runderlass „Personenbezogene Daten von Lehrkräften in Akten der Schule“ v. 21.08.1992; Runderlass „Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule“ v. 19.01.2018.
- Rheinland-Pfalz: § 67 SchulG-RLP; § 89 (Verarbeitung personenbezogener Daten); § 33 Abs. 4 SchulO RP 2009 (Teilnahme am Unterricht und an sonstigen Schulveranstaltungen), § 89 SchulO RP 2009 (Verarbeitung personenbezogener Daten), § 90 SchulO RP 2009 (Sicherung und Aufbewahrung personenbezogener Daten); § 49 GrundSchulO-RLP 2008 (Erhebung und Verarbeitung personenbezogener Daten), § 50 GrundSchulO-RLP 2008 (Sicherung und Aufbewahrung personenbezogener Daten); § 55 BBiSchulO RP (Erhebung und Verarbeitung personenbezogener Daten), § 56 BBiSchulO RP (Sicherung und Aufbewahrung personenbezogener Daten); §§ 11 Abs. 6, 22 Abs. 2, 23 Abs. 2 SchulO für den inklusiven Unterricht.
- Saarland: insbesondere § 20b SchoG SL (Verarbeitung von personenbezogenen Daten unter Hinweis auf die Vorschriften des Schulwesen-Datenschutzgesetzes), ferner § 20a SchoG SL (Schulpsychologischer Dienst), § 20c (Wissenschaftliche Forschung) § 20db SchoG SL (Durchführung laufender Landesstatistiken), § 20e SchoG SL (Qualitätsentwicklung und Qualitätssicherung); § 3 SchulwDSG SL (Rechtmäßigkeit); § 4 SchulwDSG SL (Besondere Ziele); § 5 SchulwDSG SL (Umfang der Verarbeitung); § 6 SchulwDSG SL (Verarbeitung mit Profilingmöglichkeit); § 7 SchulwDSG SL (Übermittlung); § 8 SchulwDSG SL (Veröffentlichung von Berichten, Akteneinsicht); § 9 SchulwDSG SL (Aufbewahrungs- und Speicherdauer); § 10 SchulwDSG SL (Datensicherheit); § 11 SchulwDSG SL (Verantwortlichkeit); vollständig SchulwDSV SL.
- Sachsen: § 63a SächsSchulG (der in Abs. 1 auf die DS-GVO und das SächsDSDG verweist) i.V.m. Ziffer I und II VwV Schuldatenschutz Sachsen (Sonderregelungen in §§ 5 Abs. 5, 15 Abs. 2, 31 Abs. 3 und 4, 63b SächsSchulG).
- Sachsen-Anhalt: § 84a SchulG LSA (insbesondere § 84a Abs. 1 und 2 SchulG LSA).
- Schleswig-Holstein: § 30 SchulG SH (insbesondere Abs. 1) i.V.m. SchulDSVO SH und Anlage 2 SchulDSVO SH (Sonderregelungen in §§ 31, 32 SchulG SH zur Datenübermittlung bei volljährigen Schülern und zu wissenschaftlicher Forschung, Praktika und Prüfungsarbeiten im Rahmen der Lehrkräfteausbildung).
- Thüringen: § 57 ThürSchulG (insbesondere Abs. 1); § 47 ThürASObbS und § 136 ThürSchulO (Datenerfassung in Schülerbögen sowie Klassen- und Kursbüchern).

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht (insbesondere Nr. 4 zu den Rechtsgrundlagen und Nr. 6 zum Umfang der Datenverarbeitung)
- ISO/IEC 27701:2025 Ziff. B.3.13 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

Nr. 5.3 – Besondere Kategorien personenbezogener Daten
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

Kriterium

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung von besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO offensichtlich unrechtmäßig i.S.v. Art. 9 Abs. 2 DS-GVO ist.
2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung mit Blick auf Art. 9 DS-GVO rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

Erläuterung

Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO ist grundsätzlich untersagt. Hiervon erfasst werden personenbezogene Daten, aus denen die rassische[36] und ethnische Herkunft (z. B. regional begrenzte Sprachen, nicht aber die Staatsangehörigkeit), politische Meinungen (z. B. Parteimitgliedschaft), religiöse oder weltanschauliche Überzeugungen (z. B. Zugehörigkeit zu einer Religionsgemeinschaft oder Atheist) oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten (Art. 4 Nr. 13 DS-GVO), biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art. 4 Nr. 14 DS-GVO; dies erfasst nicht einfache Lichtbilder, s. EG 51 S. 3 DS-GVO), Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO) oder Daten zum Sexualleben oder der sexuellen Orientierung (z. B. Informationen zu Hetero-, Bi- Homo- und Transsexualität; zu den Datenarten s.a. Begleitdokument Risikobewertungskonzept).

Eine Verarbeitung ist im Rahmen der in Art. 9 Abs. 2 DS-GVO aufgeführten Ausnahmen zulässig. Da eine Einwilligung (wie in den Erläuterungen zu Nr. 5.2) als Erlaubnistatbestand für eine Verarbeitung regelmäßig ausscheidet, kommen vor allem die Erlaubnistatbestände der Art. 9 Abs. 2 lit. b, g und h DS-GVO in Betracht. Diese verlangen eine Grundlage im Unionsrecht oder im Recht der Mitgliedstaaten. Im Kontext schulischer Informationssysteme sind dabei insbesondere die schuldatenschutzrechtlichen Vorschriften der Länder relevant, so sie eine Verarbeitung besonderer Kategorien personenbezogener Daten erlauben.

Landesgesetzliche Regelungen

Vorgaben zur Verarbeitung besonderer Kategorien personenbezogener Daten finden sich insbesondere in den folgenden landesrechtlichen Vorschriften. Soweit in einzelnen Ländern keine spezifischen schuldatenschutzrechtlichen Vorschriften bestehen, gelten die allgemeinen datenschutzrechtlichen Vorschriften (insbesondere die DS-GVO und die ergänzenden allgemeinen Landesdatenschutzgesetze).

- Baden-Württemberg: Im SchulG selbst finden sich keine relevanten spezifischen Vorschriften zur Verarbeitung besonderer Kategorien personenbezogener Daten. Nach Ziff. 1.4 VwV-Datenschutz an öffentlichen Schulen BW ist die nach Art. 9 DS-GVO erforderliche Vorschrift für die Verarbeitung sensibler Daten in der aufgrund von § 115 SchulG BW erlassenen SchulStat-DVV BW zu finden. Diese bezieht sich aber nur allgemein auf statistische Erhebungen und bestimmte Übermittlungen zwischen Schulen. Zusätzlich zu berücksichtigen sind Ziff. 1.9.1. VwV-Datenschutz an öffentlichen Schulen BW zur DSFA,

[36] Die Verwendung des Begriffs „rassische Herkunft" bedeutet gemäß EG 51 S. 2 DS-GVO nicht, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt.

wenn sensible Daten verarbeitet werden, und Ziff. 1.10.2. VwV-Datenschutz an öffentlichen Schulen BW, wenn es um eine Meldung von Datenschutzverletzungen geht. Zudem greift Ziff. 2.3. VwV-Datenschutz an öffentlichen Schulen BW, wenn es um die Übermittlung besonderer Kategorien personenbezogener Daten geht.

- Bayern: Besondere Kategorien personenbezogener Daten werden in § 85 Abs. 1 und § 85a Abs. 2 Nr. 1 lit. a BayEUG zwar nicht explizit erwähnt, von Schülerinnen und Schülern und ihren Erziehungsberechtigten sowie Lehrkräften und unterrichtendem Personal dürfen aber die Religionszugehörigkeit und der Migrationshintergrund verarbeitet werden.
- Berlin: Gemäß § 64 Abs. 1 SchulG-BE dürfen von Schülerinnen und Schülern, Schulpflichtigen, ihren Erziehungsberechtigten, Lehrkräften und sonstigen schulischen Mitarbeitenden nur besonderen Kategorien personenbezogener Daten verarbeitet werden, die sich auf die Familiensprache, die Religions- und Weltanschauungszugehörigkeit oder die Gesundheit der betroffenen Personen beziehen.
- Brandenburg: § 65 Abs. 11 Nr. 7 BbgSchulG i.V.m. § 1 Abs. 2 DSV-BBG enthalten Vorgaben zur Verarbeitung von Daten über gesundheitliche Beeinträchtigungen und körperliche Behinderungen; zudem sind die Anlagen der DSV-BBG zu berücksichtigen, die die zur Verarbeitung zugelassenen personenbezogenen Daten aufführen, u.a. Anlage 1 Ziff. 1.8 DSV-BBG zu Angaben zu gesundheitlichen Beeinträchtigungen.
- Bremen: Gemäß § 2 Abs. 1 BremSchulDSG dürfen von Einzuschulenden, Schülerinnen und Schüler und Schulbewerberinnen und -bewerbern sowie deren Erziehungsberechtigten nur besondere Kategorien personenbezogener Daten verarbeitet werden, die sich auf Religionszugehörigkeit, Staatsangehörigkeit, Geburtsort, Jahr des Zuzugs nach Deutschland, Verkehrssprache oder Gesundheit der betroffenen Personen beziehen.
- Hessen: Gemäß § 83 Abs. 1 Satz 1 SchulG-HE dürfen Schulen Daten der besonderen Kategorien von Schülerinnen und Schülern und deren Eltern, künftig schulpflichtig werdenden oder vom Schulbesuch zurückgestellten Kindern und Jugendlichen und deren Eltern, zum Schulbesuch berechtigten Kindern und Jugendlichen und deren Eltern sowie Lehrkräften und sonstigen in der Schule beschäftigten Personen verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. § 24 SchDSV-HE betrifft die Verarbeitung von Gesundheitsdaten im Bereich sonderpädagogischer Förderung.
- Mecklenburg-Vorpommern: Gemäß § 70 Abs. 3 SchulG M-V dürfen von Schülerinnen und Schülern von den besonderen Kategorien personenbezogener Daten nur Gesundheitsdaten, Migrationshintergrund und Religionszugehörigkeit verarbeitet werden, soweit dies zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation, sowie der Schulaufsicht erforderlich ist.
- Niedersachsen: § 31 Abs. 10 NSchulG (Verarbeitung besonderen Kategorien personenbezogener Daten) regelt, dass die besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO nur für bestimmte Zwecke aufgrund der Regelungen in § 31 Abs. 1-3 NSchulG verarbeitet werden dürfen.
- Nordrhein-Westfalen: Nach § 122 Abs. 1 Satz 2 SchulG NRW beruhen § 120 und § 121 u.a. auf Art. 9 Abs. 2 lit. g DS-GVO. VO-DV I NRW (u.a. Verarbeitung von Konfession, Herkunftssprache, Art des Notfalls (Notfallinformationen), gesundheitliche Beeinträchtigung und/oder körperliche Behinderung); VO-DV II NRW (u.a. Konfession, Behinderung).
- Rheinland-Pfalz: §§ 11 Abs. 6, 22 Abs. 2, 23 Abs. 2 SchulO für den inklusiven Unterricht.
- Saarland: § 20a SchoG SL (Datenverarbeitung durch den Schulpsychologischen Dienst).
- Sachsen: §§ 5 Abs. 5, 15 Abs. 2 und 63a Abs. 2 SächsSchulG (Erwähnung Art. 9 DS-GVO Zusammenhang mit Einwilligung bzgl. Ermittlung des Entwicklungsstandes in Grund- und Förderschulen, Schulversuchen und der Verarbeitung von Kotaktdaten von Schülerinnen und Schülern, um eine Beratung durch die Agenturen für Arbeit etc. zu unterstützen); Sächsische VwV Schulpsychologische Beratung.
- Sachsen-Anhalt: § 84a Abs. 3 und 9 SchulG LSA (Verarbeitung von Gesundheitsdaten).

- Schleswig-Holstein: § 30 Abs. 4 SchulG SH (Übermittlung Gesundheitsdaten), § 32 Abs. 2 SchulG SH (Praktika und Prüfungsarbeiten im Rahmen der Lehrkräfteausbildung).
- Thüringen: § 57 Abs. 3 ThürSchulG (Verarbeitung von Gesundheitsdaten zur Schulgesundheitspflege); § 47 ThürASObbS und § 136 ThürSchulO (Datenerfassung in Schülerbögen sowie Klassen- und Kursbüchern, die auch Art. 9-Daten umfassen kann, z. B. Religionszugehörigkeit und Gesundheitsdaten).

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 17 Besondere Kategorien personenbezogener Daten
- ISO/IEC 27701:2025 Ziff. B.2.2.3 Ziele der Organisation
- ISO/IEC 27701:2025 Ziff. B.2.2.5 Verstoßende Anweisungen

Nr. 5.4 – Übermittlung personenbezogener Daten
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

Kriterium

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Übermittlung personenbezogener Daten offensichtlich rechtswidrig ist.
2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Übermittlung personenbezogener Daten rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

Erläuterung

Die schuldatenschutzrechtlichen Vorschriften der Länder enthalten Anforderungen an die Übermittlung personenbezogener Daten (d.h. an die gezielte Weitergabe an Empfänger). Diese Vorschriften unterscheiden dabei zumeist zwischen Übermittlungen an öffentliche und an nicht-öffentliche Stellen, etwa für das Führen zentraler Karteien von Schülerinnen und Schülern, für Statistiken oder für wissenschaftliche Auswertungen; vgl. insofern die Anforderungen der folgenden Landesgesetze.

Übermittlungen sind zu protokollieren, s. Nr. 3.7 Abs. 4.

Landesgesetzliche Regelungen

Vorgaben zur Übermittlung personenbezogener Daten finden sich insbesondere in den folgenden in landesrechtlichen Vorschriften. Soweit in einzelnen Ländern keine spezifischen schuldatenschutzrechtlichen Vorschriften bestehen, gelten die allgemeinen datenschutzrechtlichen Vorschriften (insbesondere die DS-GVO und die ergänzenden allgemeinen Landesdatenschutzgesetze).

- Baden-Württemberg: Ziffer 1.3.3, Ziffer 1.5.7, Ziffer 2.3, insbesondere Ziffer 2.3.1, 2.3.5 und 2.3.6 VwV-Datenschutz an öffentlichen Schulen BW (zudem wird in der VwV-Datenschutz an öffentlichen Schulen BW auf § 6 LDSG BW verwiesen); SchulStat-DVV BW, siehe insbesondere § 3 SchulStat-DVV BW bezüglich der Pseudonymisierung von Daten bei der Übermittlung.
- Bayern: Zentrale Befugnisnorm für die Übermittlung personenbezogener Daten ist Art. 85 Abs.1 und 2 BayEUG; für Übermittlungen personenbezogener Daten aus dem in Art. 85a Abs. 1 BayEUG genannten automatisierten Verfahren gilt darüber hinaus Art. 85a Abs. 3 BayEUG.
- Berlin: § 64 Abs. 3-8 u. 10 SchulG-BE, § 65 (siehe insbesondere Abs. 3 Satz 5) SchulG-BE; §§ 15, 18 Abs. 4 u. 5, 24-28 SchulDatenV Berlin; § 2 Abs. 4 i.V.m. den Anlagen der DigLLV.
- Brandenburg: § 65 Abs. 2, 6, 7, 8, § 65a Abs. 2 u. 3 BbgSchulG; § 6, § 7, § 11 Abs. 4, § 13, § 17 Abs. 2 DSV-BBG.

- Bremen: Für öffentliche Stellen: §§ 5-9 BremSchulDSG; für nicht-öffentliche Stellen § 10 BremSchulDSG.
- Hamburg: Für Schulportale und andere pädagogische Netzwerke: § 98b Abs. 2 insbesondere Satz 5 und 6 HmbSG, § 1 Abs. 3 Satz 2 SchulDSV HA; für öffentliche Stellen: § 1 Abs. 3 Satz 2 SchulDSV HA, § 1 Abs. 4 SchulDSV HA, § 6 Abs. 2 SchulDSV HA.
- Hessen: § 83 Abs. 1 Satz 4, Abs. 7 und 8, § 85 SchulG-HE; § 21 Abs. 1 und 2, §§ 22, 23, 31, 35, 37 SchDSV-HE.
- Mecklenburg-Vorpommern: Für Schulen, Schulträger und Schulbehörden: § 70 Abs. 4 SchulG M-V; §§ 3 und 4 SchulDSVO M-V; zur Synchronisierung von digitalen Schuldiensten, Lern- und Lehrinhalten mit dem mecklenburg-vorpommerischen IDM: § 5a Abs. 4 und 5 SchulDSVO M-V.
- Niedersachsen: § 31 NSchulG, insbesondere sind die § 31 Abs. 2-4 NSchulG Rechtsgrundlagen der Schulen für die Übermittlung von personenbezogenen Daten an Dritte, die diese Daten teilweise ausdrücklich ersuchen müssen.
- Nordrhein-Westfalen: § 120 Abs. 7 Satz 1 SchulG NRW (Datenübermittlungen an eine Schule, die Schulaufsichtsbehörde, den Schulträger etc.); § 120 Abs. 7 Satz 2 SchulG NRW (Datenübermittlungen an andere öffentliche Stellen); § 120 Abs. 7 Satz 3 SchulG NRW (Datenübermittlungen an nicht-öffentliche Stellen); § 120 Abs. 8 SchulG NRW (Datenübermittlungen zu Planungs- und Statistikzwecken); s.a. § 121 Abs. 2-6 SchulG NRW zur Übermittlung von Personaldaten; § 5 VO-DV I NRW (Allgemeine Bestimmungen für die Übermittlung von Daten), § 6 VO-DV I NRW (Datenübermittlung bei einem Schulwechsel), § 7 VO-DV I NRW (Datenübermittlung zum Zwecke der Schulpflichtüberwachung sowie zur Sicherstellung der Teilnahme an Ausbildung und Ausbildungsvorbereitung), § 8 VO-DV I NRW (Datenübermittlung zum Zwecke der Schulgesundheitspflege); § 8 VO-DV II NRW (Datenübermittlungen).
- Rheinland-Pfalz: Für den öffentlichen Bereich: § 67 Abs. 1 Satz 2, Abs. 3 Satz 4, Abs. 5, Abs. 9 SchulG-RLP; für den nicht-öffentlichen Bereich: § 67 Abs. 6 SchulG-RLP; § 89 Abs. 4 bis 8 SchulO RP 2009 im Schulkontext; § 49 Abs. 5 bis 7 GrSchulO RP 2008 im Schulkontext; § 55 Abs. 5 bis 8 BBiSchulO RP im Schulkontext.
- Saarland: § 7 SchulwDSG SL (Übermittlung personenbezogener Daten); §§ 21 bis 29 SchulwDSV SL (Übermittlung personenbezogener Daten).
- Sachsen: § 63a Abs. 2 SächsSchulG (Übermittlung von Kontaktdaten mit Einwilligung an die Agenturen für Arbeit, die Jobcenter und die örtlichen Träger der öffentlichen Jugendhilfe); § 63b SächsSchulG i.V.m. SächsSchulStatVO (Statistik); Nr. 6 Sächsische VwV Schulpsychologische Beratung.
- Sachsen-Anhalt: Für öffentliche Stellen: § 84a Abs. 7 Satz 2, Abs. 8 SchulG LSA; für nicht-öffentliche Stellen: § 84a Abs. 8 Satz 2 SchulG LSA; für Gesundheitsdaten: § 84a Abs. 9 SchulG LSA; für Statistikzwecke: § 84d SchulG LSA; Ziffer 4 Runderlass „Richtlinien zum Schülerstammblatt und zum sonstigen Datenbestand allgemeinbildender Schulen, berufsbildender Schulen und Schulen des Zweiten Bildungsweges des Landes Sachsen-Anhalt“.
- Schleswig-Holstein: Für öffentliche Stellen (nicht Gesundheitsdaten i.S.v. Art. 9 DS-GVO): § 30 Abs. 3 SchulG SH; für öffentliche Stellen (Gesundheitsdaten i.S.v. Art. 9 DS-GVO): § 30 Abs. 4 SchulG SH; Übermittlung bzgl. Berufsschulpflicht: § 30 Abs. 8 SchulG SH; für Datenübermittlung per E-Mail: § 9 SchulDSVO SH.
- Thüringen: § 136 Abs. 7a ThürSchulO (Datenübermittlung an die Agentur für Arbeit); § 137 Abs. 2 ThürSchulO und § 48 ThürASObbS (Datenübermittlung bei Schulwechsel).

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2025 Ziff. B.2.2.3 Ziele der Organisation
- ISO/IEC 27701:2025 Ziff. B.2.2.5 Verstoßende Anweisungen

- ISO/IEC 27701:2025 Ziff. B.2.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten

Nr. 5.5 – Löschung, Aufbewahrung, Berichtigung und Einsichtnahme
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

Kriterium

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung offensichtlich gegen Löschungs- und/oder Aufbewahrungspflichten der Schulen, Schulbehörden und Schulträger, gegen Berichtigungspflichten und gegen Pflichten auf Gewährung von Einsicht verstößt.

2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Verarbeitung mit Blick auf Löschungs-, Aufbewahrungs-, Berichtigungs- und Einsichtspflichten rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

Erläuterung

Den Schulen, Schulbehörden und Schulträgern als Verantwortliche und System-Kunden werden durch die für den Bereich der Schule relevanten landesgesetzlichen Regelungen verschiedene Pflichten auferlegt. Hierzu gehören die Einhaltung von Lösch- und Aufbewahrungspflichten, Berichtigungspflichten sowie die Erfüllung gesetzlicher Pflichten zur Gewährung von Einsichtnahmen. Zur Erfüllung dieser Pflichten ist der System-Kunde auf die Mitwirkung des System-Anbieters als Auftragsverarbeiter angewiesen, da der System-Anbieter häufig einen besseren Einblick in die relevanten Verarbeitungsvorgänge sowie Zugriff auf die ggf. benötigten technischen Einrichtungen hat. Diese Mitwirkungspflichten des System-Anbieters ändern indes nichts an der Pflicht des System-Kunden, die genannten Pflichten einzuhalten. Eine Pflichtendelegation vom System-Kunden auf den System-Anbieter findet nicht statt. Der System-Anbieter hat den System-Kunden aber nach Kräften bei der Wahrnehmung der Pflichten zu unterstützen.

Personenbezogene Daten sind durch die Schulen, Schulbehörden und Schulträger nach der überwiegenden Mehrheit der Landesschulgesetze zu löschen, sobald die Verarbeitung nicht mehr zur Erfüllung ihrer Aufgaben (Erfüllung des Bildungs- und Erziehungsauftrages) erforderlich ist. Ggf. sind Aufbewahrungsfristen aus den Landesschulgesetzen bzw. zugehörigen Rechtsverordnungen zu beachten.[37]

Daneben sind die Schulen, Schulbehörden und Schulträger ggf. verpflichtet, Berichtigungen an personenbezogenen Daten vorzunehmen. Dies hat dann auch im Datenbestand des System-Anbieters zu erfolgen, weshalb dieser explizit bei der Richtigstellung mitzuwirken hat. Zudem hat er Berichtigungsanliegen, die an ihn gerichtet werden, aber auch den Datenbestand der Schulen, Schulbehörden und Schulträger betreffen, an diese weiterzugeben und insofern bei der Berichtigung mitzuwirken.

Schließlich können verschiedene Pflichten des Verantwortlichen zur Gewährung von Einsichtnahmen bestehen. Diese können auch an Auftragsverarbeiter ausgegliederte Verarbeitungsvorgänge betreffen, weshalb der System-Anbieter bei der Erfüllung dieser Pflicht mitzuwirken hat.

Landesgesetzliche Regelungen

Vorgaben zur Löschung, Aufbewahrung, Berichtigung und Einsichtnahme finden sich insbesondere in den folgenden in landesrechtlichen Vorschriften. Soweit in einzelnen Ländern keine spezifischen schuldatenschutzrechtlichen Vorschriften bestehen, gelten die allgemeinen datenschutzrechtlichen Vorschriften (insbesondere die DS-GVO und die ergänzenden allgemeinen Landesdatenschutzgesetze).

- Baden-Württemberg: § 115 Abs. 3a SchulG BW; Ziffer 1.5, Ziffer 2.5.3. VwV-Datenschutz an öffentlichen Schulen BW (Löschung und Löschfristen); Ziffer 2.6. VwV-Datenschutz an öffentlichen Schulen BW (Einsichtnahme in Prüfungsarbeiten); Ziffer 3.2 VwV-Datenschutz an öffentlichen Schulen BW (Löschung von Daten von Lehrkräften).

[37] DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 16 f.

- Bayern: § 40 BaySchO (Aufbewahrungsfristen); § 41 BaySchO (Einsichtnahme); Art. 85a Abs. 4, Art. 113a Abs. 4, Art. 113b Abs. 4 Satz 2, Art. 113c Abs. 3 Satz 9 BayEUG (Löschung).
- Berlin: § 5 SchulDatenV Berlin (Einsichtnahme); § 16 SchulDatenV Berlin (Aufbewahrungs- und Löschfristen); § 2 Abs. 6, § 3 Abs. 2 u. 3, § 5 Abs. 5 DigLLV Berlin (Löschung).
- Brandenburg: § 10 (Einsichtnahme), § 12, 14 Abs. 6 DSV-BBG (Löschung).
- Bremen: § 3, § 4 Abs. 2 BremSchulDSG; Richtlinie über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in öffentlichen Schulen der Stadtgemeinde Bremen.
- Hamburg: §§ 2, 4 SchulDSV HA.
- Hessen: Videoaufzeichnungen § 83 Abs. 6 SchulG-HE; § 16, § 17 i.V.m. Anlage 3, § 21 Abs. 3 SchDSV-HE.
- Mecklenburg-Vorpommern: § 70 Abs. 6 Nr. 4 SchulG M-V i.V.m. §§ 5, 6 Abs. 6 SchulDSVO M-V.
- Niedersachsen: Runderlass „Aufbewahrung von Schriftgut in öffentlichen Schulen; Löschung personenbezogener Daten“.
- Nordrhein-Westfalen: § 120 Abs. 9 und 10 SchulG NRW (Auskunft), § 121 Abs. 3 SchulG NRW (Löschung statistischer Daten); § 3 VO-DV I NRW (Berichtigung, Auskunft, Einsicht in Akten), § 9 VO-DV I NRW (Aufbewahrung, Aussonderung, Löschung und Vernichtung der Dateien und Akten); § 4 Abs. 7 VO-DV I NRW (bzgl. Schultagebüchern).
- Rheinland-Pfalz: § 90 SchulO RP 2009 (Sicherung und Aufbewahrung personenbezogener Daten); § 50 GrSchulO RP 2008 (Sicherung und Aufbewahrung personenbezogener Daten); § 56 BBiSchulO RP (Sicherung und Aufbewahrung personenbezogener Daten).
- Saarland: § 20b Abs. 4, § 20e Abs. 2 SchoG SL; § 8 SchulwDSG SL (Veröffentlichung von Berichten, Akteneinsicht); § 9 SchulwDSG SL (Aufbewahrungs- und Speicherdauer).
- Sachsen: Ziffer III Nr. 3 und 9 und Ziffer IV VwV Schuldatenschutz Sachsen (Löschung personenbezogener Daten, Betroffenenrechte).
- Sachsen-Anhalt: § 84a Abs. 10 SchulG LSA (Erforderlichkeit und Aktenkundigkeit), § 84e Abs. 2 und Abs. 3 SchulG LSA (Löschung); Ziffer 9 und 10 Runderlass „Richtlinien zum Schülerstammblatt und zum sonstigen Datenbestand allgemeinbildender Schulen, berufsbildender Schulen und Schulen des Zweiten Bildungsweges des Landes Sachsen-Anhalt“.
- Schleswig-Holstein: § 30 Abs. 9 SchulG SH; §§ 10 und 19 SchulDSVO SH.
- Thüringen: § 136 Abs. 9, 10 ThürSchulO; § 47 Abs. 10, 11 ThürASObbS.

Aufbewahrungspflichten finden sich in fast allen Schulgesetzen der Länder. Hierin werden Aufbewahrungspflichten für verschiedene Unterlagen vorgeschrieben. Für einen grundlegenden Überblick über die Lösch- und Aufbewahrungsfristen siehe die Anlage Aufbewahrungs- und Löschfristen der Landesgesetze in Jahren.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht
- SDM-Baustein 60 „Löschen und Vernichten“
- ISO/IEC 27701:2025 Ziff. B.2.2.3 Ziele der Organisation
- ISO/IEC 27701:2025 Ziff. B.2.2.5 Verstoßende Anweisungen
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 6 – Sicherstellung der Vertraulichkeit und Einhaltung der datenschutzrechtlichen Anforderungen beim Personal

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DS-GVO)

Kriterium

1) Der System-Anbieter richtet einen Prozess ein, um sicherzustellen, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen des System-Anbieters vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit gemäß der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung und zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

2) Der Prozess umfasst auch die Dokumentation der Verpflichtungserklärungen sowie ihre Anpassungen, wenn sich Zugriffs- und Verarbeitungsbefugnisse ändern.

Erläuterung

Die Verpflichtung zur Vertraulichkeit fördert das Gewährleistungsziel der Vertraulichkeit (SDM C1.4). Sie erfolgt bei allen Mitarbeitenden, die personenbezogene Daten verarbeiten. Zur Verpflichtung gehört auch eine Belehrung über die sich ergebenden Pflichten aus dem Datenschutzrecht.

Siehe hierzu die Erläuterung zu Nr. 1.6.

Umsetzungshinweis

Seinen Mitarbeitenden sollte der System-Anbieter eine Ausfertigung des Verpflichtungstextes mitsamt den Hinweisen auf mögliche Folgen von Verschwiegenheitspflichtverletzungen aushändigen. Die DSK hat hierfür einen Mustertext entwickelt.[38]

Der System-Anbieter sollte die Mitarbeitenden in regelmäßigen Zeitintervallen, etwa im Zusammenhang mit Schulungen oder bei einem Aufgabenwechsel, daran erinnern, dass sie zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet sind. Außerdem sollte der System-Anbieter Mitarbeitende zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit regelmäßig sensibilisieren.

In der Dokumentation des Prozesses sollte der System-Anbieter Festlegungen treffen, wer für die Vornahme der Verpflichtung verantwortlich ist, wer sie wann und in welcher Weise durchführt, welche Personen zu welchem Zeitpunkt verpflichtet werden müssen und welcher Nachweis über die Verpflichtung wo und wie lange aufbewahrt wird.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 27002:2022 Ziff. 6.2 Beschäftigungs- und Vertragsbedingungen
- ISO/IEC 27002:2022 Ziff. 6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- ISO/IEC 27701:2025 Ziff. B.3.18 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Nr. 7 – Unterstützung des System-Kunden bei der Wahrung der Betroffenenrechte

Erläuterung

Für die Erfüllung der Rechte der betroffenen Personen nach Kapitel III der DS-GVO (Art. 12 ff. DS-GVO) ist der System-Kunde als Verantwortlicher zuständig. Der System-Anbieter als Auftragsverarbeiter hat den System-Kunden dabei gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e DS-GVO nach

[38] Siehe DSK, Kurzpapier Nr. 19, S. 4 f.

Möglichkeit mit geeigneten TOM zu unterstützen, damit der System-Kunde seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachkommen kann.

Nr. 7.1 – Transparente Information und Kommunikation sowie Fristen bei der Bearbeitung von Anträgen der betroffenen Personen, bei Untätigkeit oder verzögerter Bearbeitung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 12 Abs. 1 bis 4 und Art. 15 bis 22 DS-GVO)

Kriterium

1) Der System-Anbieter richtet für den System-Kunden eine Kontaktstelle ein, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Unterstützung bei der Umsetzung der Betroffenenrechte gewährleistet.

2) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, der betroffenen Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache alle notwendigen Informationen gemäß Art. 13 bis 22 DS-GVO zur Verfügung zu stellen und der betroffenen Person die Ausübung der Rechte nach Art. 15 bis 22 DS-GVO zu erleichtern.

3) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, die betroffene Person über die auf Antrag gemäß den Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, zu informieren. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

4) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, die betroffene Person zu informieren, falls der System-Kunde ihren Antrag nach Art. 15 bis 22 DS-GVO nicht rechtzeitig, spätestens innerhalb eines Monats beantworten kann. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

5) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, die betroffene Person spätestens innerhalb eines Monats darüber zu informieren, dass der System-Kunde keine Maßnahmen ergreift, um auf einen Antrag nach Art. 15 bis 22 DS-GVO hin tätig zu werden. Die Information der betroffenen Person bezieht sich auf die Gründe der Untätigkeit des System-Kunden und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

Erläuterung

Die Unterstützungspflicht des System-Anbieters besteht gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e DS-GVO „angesichts der Art der Verarbeitung" nur „nach Möglichkeit". Die Formulierung „nach Möglichkeit" bedeutet zunächst, dass dem System-Anbieter nichts Unmögliches abverlangt werden darf.[39] Die Unterstützungspflicht muss das Aufgabenspektrum des System-Anbieters betreffen und technisch leistbar sein.[40] Sie muss auch rechtlich zulässig sein.[41] Nicht entscheidend ist, ob die Unterstützung für den System-Anbieter mit einem großen Aufwand einhergeht. So dies der Fall ist, kann sich der System-Anbieter sein Tätigwerden aber vergüten lassen (s. Nr. 2.7).[42]

Konkret kann die Art der Unterstützung sehr unterschiedlich sein. Sie kann ggf. lediglich darin bestehen, „alle eingegangenen Anfragen umgehend weiterzuleiten und/oder dem Verantwortlichen [d.h. dem System-Kunden] die Möglichkeit zu geben, die einschlägigen personenbezogenen Daten direkt zu extrahieren und zu verwalten". Unter Umständen können dem System-Anbieter aber auch „spezifischere technische Aufgaben übertragen [werden], insbesondere wenn er in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten."[43] Die Einzelheiten der vom

[39] BeckOK Datenschutzrecht/*Spoerr*, Art. 28 DS-GVO Rn. 74.
[40] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 70.
[41] Paal/Pauly/*Martini*, Art. 28 DS-GVO Rn. 47: „nur iRd rechtlich und tatsächlich Möglichen".
[42] S. Ehmann/Selmayr/*Bertermann/Peintinger*, Art. 28 DS-GVO Rn. 30 zu gesonderten Vergütungsregelungen
[43] EDSA, Leitlinien 07/2020, Rn. 130 ff.

System-Kunden zu leistenden Unterstützungshandlungen sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung aufgeführt werden (s. Nr. 1.7).[44]

Art. 28 Abs. 3 UAbs. 1 S. 2 lit. e DS-GVO ändert nichts daran, dass der System-Kunde als Verantwortlicher die Verantwortung für die Wahrung der Betroffenenrechte trägt. „Daher sollte die Beurteilung der Frage, ob Anträge betroffener Personen zulässig sind und/oder die in der DSGVO festgelegten Anforderungen erfüllt sind, vom Verantwortlichen vorgenommen werden, und zwar entweder von Fall zu Fall oder mittels klarer Weisungen, die dem Auftragsverarbeiter im Vertrag vor Beginn der Verarbeitung erteilt werden."[45]

Gemäß Art. 12 Abs. 1 und 2 DS-GVO hat der System-Kunde der betroffenen Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache alle notwendigen Informationen gemäß Art. 13 bis 22 DS-GVO zur Verfügung zu stellen („zu übermitteln"). Er hat der betroffenen Person die Ausübung ihrer Rechte nach Art. 15 bis 22 DS-GVO zu erleichtern.

Nach Art. 12 Abs. 3 Satz 1 DS-GVO hat der System-Kunde der betroffenen Person die erforderlichen Informationen über die auf Antrag nach Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags mitzuteilen. Der System-Kunde muss daher bei jedem Antrag einer betroffenen Person nach Art. 15 bis 22 DS-GVO Stellung zur beantragten Maßnahme nehmen. Stützt sich der System-Kunde bei der Beantwortung von Anträgen auf eine (nationale) Ausnahme von der Erfüllung von Betroffenenrechten, hat er der betroffenen Person daher auch angemessen darzulegen, aus welchen Gründen er ihren Antrag teilweise oder vollständig ablehnt.

Aufgrund von Komplexität oder der Anzahl von Anträgen kann die Monatsfrist aus Art. 12 Abs. 3 Satz 1 DS-GVO um zwei Monate verlängert werden. In diesem Fall muss der System-Kunde die betroffene Person über die Fristverlängerung und die Gründe dafür gemäß Art. 12 Abs. 3 Satz 3 DS-GVO informieren. Der System-Anbieter muss den System-Kunden hierbei unterstützen. Bei elektronischer Antragstellung sollte die Unterrichtung ebenfalls elektronisch erfolgen, wenn die betroffene Person nichts Anderes verlangt.

Art. 12 Abs. 4 DS-GVO verpflichtet den System-Kunden, spätestens innerhalb eines Monats, zur Information der betroffenen Person über die Gründe, weshalb er trotz eines Antrags nach Art. 15 bis 21 DS-GVO nicht tätig wird, um dem Antrag zu entsprechen. Gründe, einem Antrag nicht zu entsprechen, sind z. B. unbegründete oder exzessive Anträge nach Art. 12 Abs. 5 Satz 2 lit. b DS-GVO. Weiterhin ist die betroffene Person nach Art. 12 Abs. 4 DS-GVO über ihre Möglichkeit zu unterrichten, eine Beschwerde bei der Aufsichtsbehörde gemäß Art. 77 DS-GVO oder gerichtlichen Rechtsbehelf gemäß Art. 79 DS-GVO einzulegen.

Umsetzungshinweis

Für eine Kontaktstelle können z. B. Mitarbeitende benannt werden, die als Ansprechpartner gegenüber den System-Kunden fungieren. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Werden Weisungen zur Umsetzung der Informationspflicht automatisiert ausgeführt (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), sollten auch entsprechende Felder implementiert sein, in denen der System-Kunde Informationen über die ergriffenen Maßnahmen, die Fristverlängerung und die Gründe hierfür bzw. die Gründe seiner Untätigkeit und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, angeben kann. Diese Interaktionen mit dem System-Kunden sollten automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Klausel 7.6 und 8 im Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021

[44] EDSA, Leitlinien 07/2020, Rn. 130 ff.
[45] EDSA, Leitlinien 07/2020, Rn. 130 ff.

- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.2 – Informationserteilung bei Erhebung personenbezogener Daten
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 13 oder 14 und Art. 5 Abs. 1 lit. a DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die betroffene Person über die Datenverarbeitung informieren kann oder dies durch den System-Anbieter vornehmen lassen kann. Dies umfasst im Fall einer Direkterhebung alle in Art. 13 Abs. 1 und 2 DS-GVO geforderten und im Fall einer Dritterhebung alle in Art. 14 Abs. 1 und 2 DS-GVO geforderten Angaben.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Informationspflicht des System-Kunden. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Informationspflicht des System-Kunden unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit“ s. die Erläuterungen von Nr. 7.1.

Werden personenbezogene Daten direkt bei der betroffenen Person erhoben (Direkterhebung), ist der System-Kunde nach Art. 13 DS-GVO verpflichtet, die betroffene Person zum Zeitpunkt der Erhebung über die Umstände der Datenverarbeitung zu informieren. Nach Art. 14 DS-GVO besteht die Informationspflicht für den System-Kunden auch, wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben werden (Dritterhebung). Die Angemessenheit der Frist zur Informationserteilung bei der Dritterhebung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit. a DS-GVO beträgt die Frist längstens einen Monat nach Erlangung der personenbezogenen Daten. Es gelten kürzere Fristen, wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet oder anderen Empfängern offengelegt werden sollen. Im ersten Fall verpflichtet Art. 14 Abs. 3 lit. b DS-GVO den System-Kunden dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall kann gemäß Art. 14 Abs. 3 lit. c DS-GVO die Information spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung der Informationspflicht automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Die Informationen haben in klarer und einfacher Sprache zu erfolgen und müssen insbesondere für Minderjährige in einer verständlichen Form zur Verfügung gestellt werden. Es muss den verschiedenen Altersstufen im schulischen Bildungswesen angemessen Rechnung getragen werden. Zudem muss sichergestellt werden, dass auch die Erziehungsberechtigten minderjähriger Schülerinnen und Schüler die Informationen erhalten.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.3 – Auskunftserteilung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 und Art. 5 Abs. 1 lit. a DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde betroffenen Personen Auskunft über die Datenverarbeitung erteilen und ihnen eine Kopie der personenbezogenen Daten zur Verfügung stellen kann oder durch den System-Anbieter vornehmen lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Auskunftserteilungspflicht des System-Kunden. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Auskunftserteilungspflicht des System-Kunden unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit“ s. die Erläuterungen von Nr. 7.1.

Der System-Kunde ist nach Art. 15 DS-GVO verpflichtet, der betroffenen Person auf Antrag Auskunft über eine Datenverarbeitung und ihre Umstände zu erteilen. Der System-Anbieter hat den System-Kunden durch TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung des Auskunftsrechts automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeilenangabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.4 – Berichtigung und Vervollständigung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 16 und Art. 5 Abs. 1 lit. d DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die Berichtigung und Vervollständigung personenbezogener Daten selbst vornehmen kann oder durch den System-Anbieter vornehmen lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Berichtigungs- und Vervollständigungspflicht des System-Kunden. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Berichtigungs- und Vervollständigungspflicht des System-Kunden unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit“ s. die Erläuterungen von Nr. 7.1.

Der System-Kunde ist nach Art. 16 DS-GVO verpflichtet, (ggf. auf Antrag) unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Der System-Anbieter ist verpflichtet, den System-Kunden durch TOM bei der Erfüllung der Rechte

betroffener Personen zu unterstützen. Die Berichtigung gemäß Art. 16 DS-GVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung des Rechts auf Berichtigung und Vervollständigung automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 61 „Berichtigen“
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.5 - Löschung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 17 Abs. 1 und Art. 5 Abs. 1 lit. c, d und e DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die Löschung personenbezogener Daten selbst vornehmen kann oder durch den System-Anbieter unverzüglich vornehmen lassen kann. Der System-Anbieter stellt sicher, dass die Löschung irreversibel erfolgt, indem er Maßnahmen ergreift, die dem Stand der Technik entsprechen.

2) Der System-Anbieter stellt durch TOM sicher, dass die Löschung von personenbezogenen Daten nicht nur im aktiven Datenbestand, sondern auch in Kopien und Datensicherungen vorgenommen wird.

3) Der System-Anbieter stellt durch TOM sicher, dass nach einer Wiederherstellung von Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

4) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Verpflichtung in Bezug auf das Recht auf Löschung. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Rechts auf Löschung unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit“ s. die Erläuterungen von Nr. 7.1.

Der System-Kunde ist nach Art. 17 Abs. 1 DS-GVO verpflichtet, personenbezogene Daten zu löschen. Der System-Anbieter ist verpflichtet, den System-Kunden durch TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM C1.7 und C1.5).

Zur Unterstützung des System-Kunden bei der Einhaltung der Löschpflichten aus den schuldatenschutzrechtlichen Vorschriften der Länder siehe Nr. 5.5.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung des Rechts auf Löschung automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Die Erstellung eines Löschkonzepts, z. B. nach DIN 66398-2016, wird empfohlen. Dieses kann die Festlegung von Löschverfahren beinhalten, mit denen es dem System-Kunden ermöglicht wird,

seinen Löschungspflichten nachzukommen. Dies sollte auch Backup- und Ausfallsicherungssysteme, einschließlich aller Vorgängerversionen der Daten, temporäre Dateien, Metadaten und Dateifragmente umfassen.

Die Löschung muss irreversibel sein, so dass Maßnahmen der logischen Löschung wie bspw. das Austragen von personenbezogenen Daten aus Verzeichnissen durch Löschbefehle nicht ausreichend, um die Anforderungen des Kriteriums zu erfüllen.

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu einem späteren Zeitpunkt als im aktiven Datenbestand gelöscht werden, z. B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Dies muss aber jedenfalls zeitnah erfolgen (z. B. innerhalb eines Monats). Die Löschung in Backup- und Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen.

Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei regelmäßig kürzere Fristen angestrebt werden sollten. Die Löschung in Backup- und Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen. Der System-Anbieter kann auch TOM verwenden, um selektive Löschungen durchzuführen, bei denen Backups zumindest teilweise gelöscht werden, um die Daten so schnell wie möglich zu löschen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“
- SDM-Baustein 60 „Löschen und Vernichten“
- ISO/IEC 27002:2022 Ziff. 8.10 Löschung von Informationen
- ISO/IEC 27040:2017 Ziff. 6.8.1 Daten-Löschung
- ISO/IEC 27555, Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen
- ISO/IEC 27701:2025 Ziff. B.2.4.3 Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten
- DIN 66398:2016 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten

Nr. 7.6 - Einschränkung der Verarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 18 Abs. 1 DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die Verarbeitung personenbezogener Daten selbst einschränken kann oder die Einschränkung durch den System-Anbieter vornehmen lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung des Rechts auf Einschränkung der Verarbeitung. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Rechts auf Einschränkung der Verarbeitung unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit“ s. die Erläuterungen von Nr. 7.1.

Der System-Kunde ist nach Art. 18 Abs. 1 DS-GVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken (s. Art. 4 Nr. 3 DS-GVO). Der Sys-

tem-Anbieter ist verpflichtet, den System-Kunden durch TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung des Rechts auf Einschränkung der Verarbeitung automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 62 „Einschränken der Verarbeitung“
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.7 - Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 19 DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen kann oder die Mitteilung durch den System-Anbieter vornehmen lassen kann, sowie die betroffene Person auf Verlangen über die Empfänger unterrichten kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit“ s. die Erläuterungen von Nr. 7.1.

Der System-Kunde ist nach Art. 19 DS-GVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Empfänger sind gemäß Art. 4 Nr. 9 DS-GVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden.

Soweit der System-Anbieter an der Offenlegung beteiligt war, ist er verpflichtet, den System-Kunden durch TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung der Mitteilungspflicht automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.8 - Datenübertragbarkeit
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 20 Abs. 1 und 2 DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die von einer betroffenen Person bereitgestellten personenbezogenen Daten entweder dieser Person oder einem anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format übermitteln kann oder durch den System-Anbieter übermitteln lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung des Rechts auf Datenübertragbarkeit. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Rechts auf Datenübertragbarkeit unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit" s. die Erläuterungen von Nr. 7.1.

Der System-Kunde ist unter den Voraussetzungen des Art. 20 Abs. 1 und 2 DS-GVO verpflichtet, auf Wunsch der betroffenen Person ihr oder einem anderen Verantwortlichen ihre bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln, sofern die Verarbeitung auf Einwilligung oder Vertrag beruht und mithilfe automatisierter Verfahren erfolgt. Der System-Anbieter sollte die ihm möglichen Formate in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung auflisten, um diesbezüglich Klarheit herzustellen.

Insbesondere sind die Daten so bereitzustellen, dass sie bei einem Schulwechsel von Schülerinnen und Schülern oder Lehrkräften oder im Fall einer Änderung der genutzten Anwendung für den Lehr- und Lernbetrieb unproblematisch in das neue Umfeld übertragen werden können, ohne dass bspw. Lernfortschritte oder andere für die schulische Ausbildung relevante Daten verloren gehen. Dies gilt allerdings nur, soweit dies technisch möglich ist, wovon in der Regel auszugehen ist, wenn es sich um dasselbe schulische Informationssystem handelt.

Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Der System-Anbieter sollte geeignete technische Funktionen innerhalb seines angebotenen Systems bereitstellen, die es ermöglichen, Daten in ein strukturiertes, gängiges und maschinenlesbares Format zu übertragen. Hierzu gehören z. B. Exportfunktionen in XML- oder JSON-Formate.

Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden. Werden Weisungen zur Umsetzung des Rechts auf Datenübertragbarkeit automatisiert (z. B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.9 - Widerspruch
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 21 Abs. 1 DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass dem System-Kunden alle Informationen zur Verfügung stehen, die erforderlich sind, damit dieser beurteilen kann, ob das Widerspruchsrecht der betroffenen Person wirksam ausgeübt worden ist.

2) Teilt der System-Kunde dem System-Anbieter mit, dass der Widerspruch wirksam ist, stellt der System-Anbieter nach Möglichkeit sicher, dass die Daten nicht mehr verarbeitet werden können. Bezieht sich der Widerspruch nur auf die Verarbeitung zu bestimmten Zwecken, stellt der System-Anbieter nach Möglichkeit sicher, dass die Daten zu diesen Zwecken nicht mehr verarbeitet werden.

3) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung des Widerspruchsrechts. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Widerspruchsrechts unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit" s. die Erläuterungen von Nr. 7.1.

Die betroffene Person hat gemäß Art. 21 Abs. 1 DS-GVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 UAbs. 1 lit. e oder f DS-GVO erfolgt, Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten daraufhin nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Hat die betroffene Person das Widerspruchsrecht wirksam ausgeübt, ist der System-Kunde mithin verpflichtet, die Verarbeitung der betroffenen personenbezogenen Daten für die Zukunft zu unterlassen.

Der System-Anbieter ist verpflichtet, den System-Kunden durch TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Daher muss der System-Anbieter dem System-Kunden alle für ihn verfügbaren Informationen bereitstellen, damit der System-Kunde über den Widerspruch entscheiden kann.

Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Der System-Anbieter sollte über ein Konzept verfügen, aus dem hervorgeht, durch welche Maßnahmen er sicherstellt, dass er dem System-Kunden alle erforderlichen Daten zur Verfügung stellen und die künftige Verarbeitung der Daten unterbinden kann.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 42 „Dokumentieren"
- ISO/IEC 27701:2025 Ziff. B.2.3.2 Einhaltung von Verpflichtungen gegenüber betroffenen Personen

Nr. 7.10 - Automatisierte Entscheidungen im Einzelfall
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 22 DS-GVO)

Kriterium

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit geeigneten TOM dabei, die Rechte und Freiheiten betroffener Personen im Fall einer automatisierten Entscheidung i.S.v. Art. 22 DS-GVO zu wahren. Dazu gehört insbesondere, dass der System-Kunde das Recht der betroffenen Person auf Erwirkung des Eingreifens einer natürlichen Person seitens des System-Kunden, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gewähren kann oder durch den System-Anbieter gewähren lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Rechte des System-Kunden im Zusammenhang mit Art. 22 DS-GVO. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung dieser Rechte des System-Kunden unterstützt.

Erläuterung

Zur Bedeutung von „nach Möglichkeit" s. die Erläuterungen von Nr. 7.1.

Gemäß Art. 22 Abs. 1 DS-GVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Sollte eine solche Entscheidung insbesondere durch Rechtsvorschrift oder Einwilligung ausnahmsweise zulässig sein (Art. 22 Abs. 2 DS-GVO), was im schulischen Kontext unwahrscheinlich ist, müssen betroffenen Personen bestimmte Rechte gewährt werden. Hierzu zählen das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört (Art. 22 Abs. 2 lit. b, Abs. 3 DS-GVO; s.a. EG 71 DS-GVO).

Umsetzungshinweis

Das Eingreifen einer natürlichen Person (d.h. eines Menschen), die zur Änderung der Entscheidung befähigt und befugt ist, ist insoweit das wichtigste Element. Zudem ist Transparenz von zentraler Bedeutung, da die Darlegung des eigenen Standpunktes und die Anfechtung der Entscheidung voraussetzt, dass nachvollziehbar ist, wie die Entscheidung zustande gekommen ist.[46]

Auf den folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 251 Rev.01 Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679

Nr. 8 – Unterstützung des System-Kunden beim Führen des Verzeichnisses von Verarbeitungstätigkeiten

(Art. 28 Abs. 3 UAbs. 1 i.V.m. Art. 30 Abs. 1 DS-GVO)

Kriterium

> Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er den System-Kunden beim Führen des Verzeichnisses von Verarbeitungstätigkeiten unterstützt. Er stellt dem System-Kunden insbesondere alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der System-Kunde für das Führen seines Verzeichnisses von Verarbeitungstätigkeiten benötigt, und aktualisiert diese Informationen anlassbezogen.

Erläuterung

Gemäß Art. 30 Abs. 1 DS-GVO ist der System-Kunde verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Der System-Anbieter hat den System-Kunden dabei zu unterstützen.

Daneben trifft den System-Anbieter gemäß Art. 30 Abs. 2 DS-GVO eine Pflicht zum Führen eines eigenen Verzeichnisses zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitungen; siehe hierzu die Kriterien in Nr. 2.3.

Umsetzungshinweis

Das Maß der erforderlichen Unterstützung ist vom Einzelfall abhängig. Der System-Anbieter hat alle Informationen, die in seinem Verantwortungsbereich vorliegen und für die Führung des Verzeichnisses von Verarbeitungstätigkeiten durch den System-Kunden erforderlich sind, dem System-Kunden zur Verfügung zu stellen. Dies kann u.a. dadurch erfolgen, dass der System-Anbieter sein Verzeichnis dem System-Kunden zur Verfügung stellt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
- DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO

[46] S. Art.-29-Gruppe, WP 251 Rev.01, S. 30 f.

Nr. 9 – Unterstützung des System-Kunden bei Erfüllung seiner Pflichten nach Art. 32 DS-GVO

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f i.Vm. Art. 5 Abs. 1 lit. f und 32 DS-GVO)

Kriterium

Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er den System-Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 DS-GVO genannten Pflichten unterstützt.

Erläuterung

Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DS-GVO sieht vor, dass der Auftragsverarbeiter (hier der System-Anbieter) den Verantwortlichen (hier den System-Kunden) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 DS-GVO genannten Pflichten unterstützt. Dies ist in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festzuhalten (s. Nr. 1.7). Da den System-Anbieter eine eigene Pflicht trifft, TOM vorzusehen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten (Nr. 1.7 und Nr. 3.1 bis Nr. 3.13) kommt dieser zusätzlichen Pflicht nur eine untergeordnete Bedeutung zu.

Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DS-GVO bedeutet insbesondere nicht, dass der System-Kunde seine eigenen Verpflichtungen zur Gewährleistung von Datensicherheit auf den System-Anbieter übertragen kann.

Umsetzungshinweis

Der System-Anbieter und der System-Kunde sollten klären, wie die Verantwortung für die geeigneten TOM verteilt wird.[47] Sollten Fragen hinsichtlich der Datensicherheit auftreten, haben sich der System-Anbieter und der System-Kunde abzustimmen.

Der System-Anbieter kann den System-Kunden z. B. durch das Einrichten einer Support-Hotline, durch Tutorials oder eine gut verständliche Bedienungsanleitung unterstützen.

Nr. 10 – Unterstützung des System-Kunden bei der Datenschutz-Folgenabschätzung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f i.V.m. Art. 35 und 36 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er den System-Kunden bei der Durchführung der Datenschutz-Folgenabschätzung unterstützt. Er stellt dem System-Kunden insbesondere alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der System-Kunde für seine Datenschutz-Folgenabschätzung benötigt.

2) Der System-Anbieter unterstützt den System-Kunden bei geplanten Abhilfemaßnahmen des System-Kunden zur Bewältigung der Risiken, die z. B. Sicherheitsvorkehrungen und sonstige Verfahren enthalten und der Sicherstellung des Schutzes von personenbezogenen Daten dienen.

Erläuterung

Soweit der System-Kunde gemäß Art. 35 DS-GVO zu einer Datenschutz-Folgenabschätzung verpflichtet ist, hat ihn der System-Anbieter durch Informationen, Analysen und Schutzmaßnahmen zu unterstützen.

Die deutschen Aufsichtsbehörden haben gemäß Art. 35 Abs. 4 DS-GVO Listen von Verarbeitungsvorgängen veröffentlicht, für die neben den Fällen des Art. 35 Abs. 3 DS-GVO eine Datenschutz-

[47] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 73.

Folgenabschätzung vom System-Kunden zwingend durchgeführt werden muss. Zu diesen Listen siehe die Anlage Listen nach Art. 35 Abs. 4 DS-GVO zur Datenschutz-Folgenabschätzung.

Umsetzungshinweis

Die Unterstützungspflichten bei der Datenschutz-Folgenabschätzung sollten am Einflussbereich des System-Anbieters ausgerichtet werden, etwa im Bereich der TOM zur Gewährleistung der Datensicherheit. Zur Einschätzung, ob ein oder welches Risiko bei den jeweiligen Verarbeitungsvorgängen des schulischen Informationssystems gegeben ist, werden Datenflussmodelle und -analysen erstellt, wenn diese nicht bereits aus der Systembeschreibung des System-Anbieters hervorgehen. Bei der Beurteilung des Risikos kann auf das Risikobewertungskonzept (siehe Begleitdokument) zurückgegriffen werden.

Der System-Anbieter sollte dem System-Kunden eine Muster-Folgenabschätzung bereitstellen können.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 248 Rev. 01 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“
- Klausel 8 im Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- DSK, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- SDM, Abschnitt D4.4.1 Plan: Spezifizieren / DSFA / Dokumentieren
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung

Nr. 11 – Nachweis der Einhaltung und Ermöglichung von sowie Mitwirkung an Überprüfungen

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO)

Kriterium

> Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er in der Lage ist, alle Informationen erbringen zu können, die für den Nachweis der Einhaltung der in Art. 28 DS-GVO enthaltenen Verpflichtungen notwendig sind, und dass er Überprüfungen, einschließlich Inspektionen, durch den Verantwortlichen oder einen anderen von diesem beauftragten Prüfer zulässt und dazu beiträgt.

Erläuterung

Um die Einhaltung der in diesem Katalog und sich unmittelbar aus Art. 28 DS-GVO ergebenden Pflichten zu gewährleisten und zu überprüfen, muss der Verantwortliche, bzw. der System-Kunde, in der Lage sein, die Einhaltung der Verpflichtungen selbständig zu überprüfen oder durch Dritte überprüfen zu lassen. Ein vertraglicher – und somit notfalls einklagbarer – Anspruch auf Überprüfung und Unterstützung (s. Nr. 1.10) bei der Überprüfung der Einhaltung dieser Verpflichtungen stärkt die Position des Verantwortlichen in dieser Aufgabe und gewährleistet damit mittelbar die Durchsetzung eines hohen Schutzniveaus für die personenbezogenen Daten der System-Nutzer.

Umsetzungshinweis

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2025 Ziff. B.2.2.6 Kundenverpflichtungen

Nr. 12 – Rückgabe und Löschung von Daten nach Abschluss der Erbringung der Verarbeitungsleistungen

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g DS-GVO)

Kriterium

> Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass die Rückgabe überlassener Datenträger, die personenbezogene Daten enthalten, sowie die Rückgabe und Löschung der beim System-Anbieter gespeicherten personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen oder nach Weisung des System-Kunden erfolgen, sofern nicht nach nationalem oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht.

Erläuterung

S.a. Nr. 1.9 zur Rückgabe und Löschung von Daten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung.

Datenträger i.d.S. sind Materialien, in oder auf denen Daten aufgezeichnet werden können und von denen Daten abgerufen werden können (ISO/IEC 2382:2015, Informationstechnik - Vokabular, Ziffer 2121321 „Datenträger“).

Umsetzungshinweis

Auf die Umsetzungshinweise unter Nr. 7.5 wird bzgl. der Löschung hingewiesen.

Alle überlassenen Datenträger des System-Anbieters sollten nach Abschluss der Erbringung der Verarbeitungsleistungen oder auf Weisung des System-Kunden nach einem formalen Managementverfahren sicher und geschützt entsorgt werden.

Die Maßnahmen aus DIN 66399 und ISO/IEC 21964-1 zur Vernichtung von Datenträgern können hinzugezogen werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 21964:2018 Informationstechnik - Bürogeräte - Vernichten von Datenträgern Teil 1 bis Teil 3
- ISO/IEC 27002:2022 Ziff. 7.10 Speichermedien
- ISO/IEC 27002:2022 Ziff. 7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
- ISO/IEC 27701:2025 Ziff. B.3.20 Speichermedien
- ISO/IEC 27701:2025 Ziff. B.3.21 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Kapitel III: Subauftragsverarbeitung

Erläuterung

Für die Auftragsverarbeitung gilt grundsätzlich das Prinzip der eigenhändigen Leistungserbringung. Unter bestimmten Voraussetzungen kann der System-Anbieter weitere Auftragsverarbeiter (sog. Subauftragsverarbeiter) in Anspruch nehmen. Soweit diese Subauftragsverarbeiter ihrerseits auf weitere Subauftragsverarbeiter zugreifen, ergeben sich mehrstufige Unterauftragsverhältnisse.

Der System-Anbieter als Hauptauftragsverarbeiter hat allerdings dafür Sorge zu tragen, dass auch der Subauftragsverarbeiter alle Pflichten erfüllt, die der System-Anbieter als Hauptauftragsverarbeiter erfüllen muss, soweit er hiervon nicht gesetzlich befreit ist. Schließlich bleibt der System-Anbieter gegenüber dem System-Kunden durchgängig für die Auftragsausführung verantwortlich.

Nr. 13 – Subauftragsverhältnisse

Nr. 13.1 – Genehmigung der Subauftragsverarbeitung, Information des System-Kunden, Einspruch
(Art. 28 Abs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter verfügt über einen definierten Prozess, der sicherstellt, dass er keine weiteren Auftragsverarbeiter (d.h. Subauftragsverarbeiter) in die Erbringung des schulischen Informationssystems einbindet, bevor der System-Kunde hierzu seine vorherige gesonderte oder allgemeine Genehmigung erteilt hat.

2) Die Genehmigung muss schriftlich erteilt werden, was auch in einem elektronischen Format erfolgen kann.

3) Im Falle einer allgemeinen Genehmigung muss der System-Anbieter den System-Kunden (also dessen befugte Mitarbeitende) über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subauftragsverarbeiters informieren und auf diese Weise dem System-Kunden die Möglichkeit geben, gegen derartige Änderungen Einspruch zu erheben. Der System-Anbieter gewährleistet, dass der System-Kunde auf jeder Stufe der Auftragsverarbeitung Gebrauch von seinem Einspruchsrecht machen kann.

4) Der System-Anbieter hat sicherzustellen, dass dem System-Kunden Informationen über alle Subauftragsverarbeiter vorliegen. Die Subauftragsverarbeiter müssen namentlich und mit ladungsfähiger Anschrift benannt werden. Die von ihnen ausgeführten Verarbeitungen müssen ebenfalls benannt werden.

Erläuterung

Der System-Anbieter als Auftragsverarbeiter kann unter den Voraussetzungen von Art. 28 Abs. 2 und 4 DS-GVO weitere Auftragsverarbeiter in die Erbringung des schulischen Informationssystems einbinden (sog. Subauftragsverarbeiter).

Nicht jeder eingesetzte Dienstleister ist zugleich ein Subauftragsverarbeiter. So liegt keine Subauftragsverarbeitung vor, wenn es beim Dienstleister an einer Verarbeitung personenbezogener Daten fehlt. Dies ist bspw. der Fall bei der Miete von Räumen in einem Rechenzentrum (Co-Location), wenn dem Dienstleister der Zugriff auf Datenverarbeitungsanlagen und personenbezogene Daten durch TOM verwehrt ist. Werden Subaufträge vergeben, hat der System-Anbieter die Qualitätssicherung und die Einhaltung des Datenschutzes in der Leistungskette zu gewährleisten. Insbesondere darf die Einbindung von Subauftragsverarbeitern nicht dazu führen, dass die Wahrung der Betroffenenrechte erschwert wird (s. Nr. 13.4).

Die vorherige Genehmigung kann gemäß Art. 28 Abs. 2 DS-GVO allgemein oder gesondert erfolgen. Bei einer allgemeinen Genehmigung gestattet der System-Kunde dem System-Anbieter allgemein oder für bestimmte Verarbeitungstätigkeiten, im Vertrag nicht näher bezeichnete Subauftragsverarbeiter einzusetzen. Bei einer gesonderten Genehmigung wird dem System-Anbieter ein konkretes Unterauftragsverhältnis mit einem konkreten Subauftragsverarbeiter erlaubt.[48]

Die Genehmigung hat schriftlich zu erfolgen, was ein elektronisches Format mit einschließt.[49] Dieses Formerfordernis verlangt keine qualifizierte Signatur i.S.v. § 126a BGB. Es genügt auch Textform i.S.v. § 126b BGB.

Der System-Anbieter hat den System-Kunden im Falle einer allgemeinen Genehmigung gemäß Art. 28 Abs. 2 Satz 2 DS-GVO zu informieren (etwa indem die Mitarbeitenden des System-Kunden informiert werden; ist der System-Kunde Schulträger, ist es nicht ausreichend, die Lehrkräfte zu informieren), bevor er Subauftragsverarbeiter hinzuzieht oder bestehende Subauftragsverarbeiter durch andere ersetzt. Der System-Kunde kann durch einen Einspruch die geplante Hinzuziehung oder Ersetzung unterbinden.[50]

[48] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 44 und 46.
[49] Zum elektronischen Format s. Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 43; DSK, Kurzpapier Nr. 13, S. 3.
[50] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 44 f.

Dem System-Kunden müssen jederzeit Informationen über alle Subauftragsverarbeiter vorliegen (also auch über von Subauftragsverarbeitern ggf. eingebundene Sub-Subauftragsverarbeiter, usw.).[51] Die Letztentscheidung über die Beauftragung eines bestimmten Subauftragsverarbeiters liegt beim System-Kunden.[52]

Umsetzungshinweis

Nach Art. 28 Abs. 2 Satz 1 DS-GVO bedarf es für die Einbindung von Subauftragsverarbeitern der Genehmigung des System-Kunden. Die Genehmigung kann gesondert oder allgemein erteilt werden. Die gesonderte Genehmigung bietet sich für solche Fälle an, in denen absehbar ist, dass Subauftragsverarbeiter nur ausnahmsweise eingesetzt werden sollen und keine Änderungen zu erwarten sind. Die allgemeine Genehmigung sollte genutzt werden, wenn bereits bei Abschluss der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung klar ist, dass zahlreiche Subauftragsverarbeiter eingesetzt werden sollen und der System-Kunde damit einverstanden ist.

Bei Massengeschäften sollten die System-Kunden bei Änderungen in den Subauftragsverarbeitungen automatisiert und proaktiv („Push"-Nachricht), z. B. über eine automatisch generierte E-Mail, informiert werden. In den AGB von System-Anbietern im Massengeschäft kann z. B. auch vorab eine Generalzustimmung für etwaige Änderungen in der Subauftragsverarbeitung, die vorbehalten werden, eingeholt werden.

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung (s. Nr. 1.8) sollten die Voraussetzungen und Folgen eines Einspruchs geregelt werden. Dies betrifft insbesondere die Frage, ob bei Einspruch die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung gekündigt werden darf.

Der System-Anbieter als Hauptauftragsverarbeiter sollte für jede Verlängerung der Auftragsverarbeitungsleistungskette eine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität inklusive ladungsfähiger Anschrift und der ausgeführten Verarbeitungen verfassen, sodass nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Systemteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden. Dies setzt voraus, dass der Subauftragsverarbeiter den System-Anbieter über seine eingebundenen Subauftragsverarbeiter informiert und die notwendigen Informationen bereitstellt (kaskadierende Informationsbereitstellung).

Zur Darstellung der involvierten Subauftragsverarbeiter eignen sich Informationsportale innerhalb oder außerhalb des angebotenen schulischen Informationssystems und ebenfalls für das proaktive Informieren („Push"-Nachricht) der System-Kunden hinsichtlich Veränderungen in der Subauftragsverarbeitung. Diese sollten fortlaufend gepflegt und aktualisiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- ISO/IEC 27701:2025 Ziff. B.2.5.7 Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden
- ISO/IEC 27701:2025 Ziff. B.2.5.8 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.2.5.9 Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

[51] EDSA, Stellungnahme 22/2024, S. 9 ff.
[52] EDSA, Stellungnahme 22/2024, S. 20.

Nr. 13.2 – Rechtsverbindliche Vereinbarung als Grundlage der Subauftragsverarbeitung
(Art. 28 Abs. 4 DS-GVO)

Kriterium

1) Der System-Anbieter stellt sicher, dass von ihm beauftragte Subauftragsverarbeiter nur auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung zwischen dem System-Anbieter und System-Kunden in Einklang steht, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass TOM so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

2) Der System-Anbieter verpflichtet seine Subauftragsverarbeiter sicherzustellen, dass ihre Subauftragsverarbeiter ebenfalls auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung zwischen dem System-Anbieter und System-Kunden in Einklang steht, und auf ihre Subauftragsverarbeiter wiederum dieselbe Verpflichtung übertragen.

Erläuterung

Wenn ein Auftragsverarbeiter (hier der System-Anbieter) die Dienste eines weiteren Auftragsverarbeiters (d.h. Subauftragsverarbeiters) in Anspruch nimmt, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen (hier des System-Kunden) auszuführen, sind diesem weiteren Auftragsverarbeiter (d.h. Subauftragsverarbeiter) gemäß § 28 Abs. 4 DS-GVO dieselben Datenschutzpflichten aufzuerlegen, die zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 DS-GVO festgelegt sind. Dabei müssen insbesondere hinreichende Garantien dafür geboten werden, dass TOM so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Die TOM des Subauftragsverarbeiters müssen also ein vergleichbares Schutzniveau wie die TOM, zu denen sich der System-Anbieter gegenüber dem System-Kunden verpflichtet hat, genügen. Dabei ist durch den Subauftragsverarbeiter die Risikoanalyse des System-Kunden nach Nr. 3.1 zu berücksichtigen.

Der System-Anbieter hat sicherzustellen, dass dieselben Verpflichtungen zwischen ihm und den Subauftragsverarbeitern, wie sie in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung oder in einem anderen Rechtsinstrument niedergelegt sind, jedem Glied der Kette der (Sub-)Subauftragsverarbeiter auferlegt sind.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- ISO/IEC 27002:2022 Ziff. 5.19 Informationssicherheit in Lieferantenbeziehungen
- ISO/IEC 27002:2022 Ziff. 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- ISO/IEC 27002:2022 Ziff. 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette
- ISO/IEC 27002:2022 Ziff. 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
- ISO/IEC 27701:2025 Ziff. B.2.5.8 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten

- ISO/IEC 27701:2025 Ziff. B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Nr. 13.3 – Auswahl und Kontrolle der Subauftragsverarbeiter
(Art. 28 Abs. 4 Satz 1 DS-GVO)

Kriterium

1) Der System-Anbieter stellt sicher, dass nur solche Auftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, welche die Gewähr für die Einhaltung der in der rechtsverbindlichen Vereinbarung über die Subauftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen bieten.

2) Der System-Anbieter stellt insbesondere sicher, dass alle von ihm beauftragten Subauftragsverarbeiter TOM so durchführen, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

3) Der System-Anbieter überzeugt sich regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen, davon, dass alle eingesetzten Subauftragsverarbeiter die in der rechtsverbindlichen Vereinbarung über die Subauftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen erfüllen.

Erläuterung

Gemäß Art. 28 Abs. 4 DS-GVO ist der Auftragsverarbeiter (hier der System-Anbieter) verpflichtet, in der rechtsverbindlichen Vereinbarung, die er mit dem Subauftragsverarbeitern abschließt, dieselben Datenschutzpflichten weiterzureichen, wie sie sich in der Vereinbarung finden, die er mit dem Verantwortlichen (hier dem System-Kunden) abgeschlossen hat. Es ist nicht erforderlich, dass die verbindliche Vereinbarung zur Subauftragsvereinbarung denselben Wortlaut hat wie die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung zwischen dem Verantwortlichen und dem Auftragsverarbeiter.[53]

Eine Pflicht zur regelmäßigen Überprüfung des Subauftragsverarbeiters (Abs. 3) ist in Art. 28 Abs. 4 DS-GVO nicht explizit aufgeführt. Allerdings steht die gesamte Zusammenarbeit zwischen Auftrags- und Subauftragsverarbeiter unter dem Vorbehalt hinreichender Garantien für die Einhaltung der Anforderungen DS-GVO. Dies verlangt nicht nur eine sorgfältige Auswahl, sondern auch eine regelmäßige Kontrolle, ob der Subauftragsverarbeiter den Anforderungen der DS-GVO noch nachkommt.[54]

Umsetzungshinweis

Der Nachweis der Gewähr für die Einhaltung der datenschutzrechtlichen Verpflichtungen kann u.a. durch Vorlage geeigneter Zertifikate oder Audits (bzw. Auditberichte) erfolgen. Soweit der System-Anbieter nicht auf Zertifikate oder Audits seiner Subauftragsverarbeiter vertrauen kann, sollte er sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter überzeugen. Dies kann durch ein zu dokumentierendes Self-Assessment des Subauftragsverarbeiters erfolgen, welches durch den System-Anbieter auf Plausibilität zu prüfen ist. In Zweifelsfällen hat der System-Anbieter weitere Prüfungen zu veranlassen.

Gemäß Art. 28 Abs. 5 DS-GVO kann die Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder eines genehmigten Zertifizierungsverfahrens (Art. 42 DS-GVO) durch einen Auftragsverarbeiter als Faktor herangezogen werden, um hinreichende Garantien i.S.v. Art. 28 Abs. 4 DS-GVO nachzuweisen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben

[53] EDSA, Stellungnahme 22/2024, S. 20 ff.
[54] S. Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 28 DS-GVO Rn. 36 zur Auftragsverarbeitung, was auf die Subauftragsverarbeitung übertragbar ist.

- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- ISO/IEC 27002:2022 Ziff. 5.19 Informationssicherheit in Lieferantenbeziehungen
- ISO/IEC 27002:2022 Ziff. 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- ISO/IEC 27002:2022 Ziff. 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette
- ISO/IEC 27002:2022 Ziff. 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
- ISO/IEC 27701:2025 Ziff. B.2.5.8 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Nr. 13.4 – Gewährleistung der Unterstützungsfunktionen
(Art. 28 Abs. 4 Satz 1 i.V.m. Art. 28 Abs. 3 UAbs. 1 Satz 2 DS-GVO)

Kriterium

Der System-Anbieter stellt sicher, dass auch bei der Einschaltung von (mehreren) Subauftragsverarbeitern seine Unterstützungsfunktionen im vereinbarten Umfang sowie seine Pflichten als Hauptauftragsverarbeiter erfüllt werden.

Umsetzungshinweis

Der System-Anbieter sollte wegen des gesteigerten Risikos bei weiteren Auftragsverarbeitungen interne Dokumentationen führen und die Verarbeitungsprozesse protokollieren. Dies dient auch der Selbstkontrolle des System-Anbieters bei der Pflichtenerfüllung auf den weiteren Auftragsstufen. Abhängig von den jeweiligen ausgelagerten Verarbeitungsprozessen sollten in der rechtsverbindlichen Vereinbarung mit dem Subauftragsverarbeiter die entsprechenden Unterstützungsfunktionen festgehalten werden. Insbesondere sollten Kontaktstellen und die jeweiligen Verantwortlichkeiten bei Subauftragsverarbeitern protokolliert und fortlaufend aktualisiert werden. Es sollten Prozesse, Meldewege und Verfahrensrichtlinien definiert und dokumentiert werden.

Unterstützungsfunktionen des System-Anbieters finden sich insbesondere in Nr. 7, Nr. 8, Nr. 9, Nr. 10; s.a. Nr. 5.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Kapitel IV: Datenverarbeitung außerhalb der EU und des EWR

Nr. 14 – Datenübermittlung an Drittstaaten und internationale Organisationen und Benennung eines Vertreters

Erläuterung

Die Zertifizierung, für die dieser Kriterienkatalog die Grundlage darstellt, ist keine Zertifizierung gemäß Art. 46 Abs. 2 lit. f DS-GVO für die internationale Übermittlung und bietet daher selbst keine angemessenen Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen. Daher ist das Zertifikat kein Übermittlungsinstrument i.S.v. Art. 46 Abs. 2 lit. f DS-GVO.

Nr. 14.1 – Angemessenheitsbeschluss, geeignete Garantien für die Datenübermittlung und Offenlegung gegenüber staatlichen Stellen von Drittländern
(Art. 45, Art. 46 und Art. 48 DS-GVO)

Kriterium

1) Der System-Anbieter übermittelt personenbezogene Daten in Drittländer oder an internationale Organisationen, sofern für den Empfängerstaat oder die internationale Organisation ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DS-GVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt, und der System-Anbieter regelmäßig, mindestens jährlich, prüft, ob der Angemessenheitsbeschluss fort gilt und die in Frage stehende Übermittlung über den benannten Beschluss erfasst wird.

2) Alternativ kann die Datenübermittlung stattfinden, wenn der System-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland oder der internationalen Organisation sicherstellt, dass die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien i.S.d. Art. 46 Abs. 2 oder 3 DS-GVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der DS-GVO gleichwertig ist.

3) Reichen nach Bewertung von Rechtslage und Praxis im Drittland oder der internationalen Organisation die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien i.S.d. Art. 46 Abs. 2 oder 3 DS-GVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der DS-GVO gleichwertig ist, ergreift der System-Anbieter zusätzliche Maßnahmen, um dieses angemessene Datenschutzniveau sicherzustellen. Andernfalls darf keine Datenübermittlung stattfinden. Der System-Anbieter muss dem System-Kunden die Bewertung von Recht und Praxis des Drittlandes oder der internationalen Organisation bereitstellen, damit der System-Kunde überprüfen kann, ob die vom System-Anbieter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in das Drittland oder an die internationale Organisation übermittelten personenbezogenen Daten gewährleisten.

4) Der System-Anbieter überwacht fortlaufend die Angemessenheit des Datenschutzniveaus und stellt sicher, dass Datenübermittlungen umgehend ausgesetzt oder beendet werden, wenn im Fall des Abs. 2 oder 3 der Empfänger die Pflichten, die er nach den geeigneten Garantien des Art. 46 Abs. 2 oder 3 DS-GVO eingegangen ist, verletzt hat oder ihre Erfüllung unmöglich ist und im Fall von Abs. 3 die zusätzlichen Maßnahmen nicht mehr eingehalten werden können oder unwirksam sind.

5) System-Anbieter, die personenbezogene Daten verarbeiten und nicht nur dem Recht der DS-GVO unterliegen, sondern zugleich dem Recht eines Drittlands, das sie zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des Drittlands verpflichtet, ergreifen zusätzliche Maßnahmen, um die personenbezogenen Daten vor einer Offenlegung an staatliche Stellen des Drittlands wirksam zu schützen. Der System-Anbieter stellt sicher, dass personenbezogene Daten staatlichen Stellen von Drittländern nur offengelegt werden, wenn die Offenlegung auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt ist. Der System-Anbieter muss den System-Kunden des schulischen Informationssystems über diese rechtliche Verpflichtung vor einer Offenlegung informieren, sofern die Information nicht aus anerkannten wichtigen Gründen des öffentlichen Interesses im EU- oder deutschen Recht verboten ist.

6) Wenn der System-Anbieter Daten an einen außerhalb der EU oder des EWR ansässigen Auftragsverarbeiter übermittelt (i.S.v. Art. 44 DS-GVO), muss er die in Kapitel V der DS-GVO festgelegten Verpflichtungen im vollen Umfang erfüllen.

Erläuterung

Übermittlungen personenbezogener Daten von betroffenen Personen in Drittländer oder an internationale Organisationen sind nur unter den in Art. 44 ff. DS-GVO genannten Voraussetzungen zulässig. Dabei müssen neben Art. 44 ff. DS-GVO auch immer die sonstigen Bestimmungen der DS-GVO eingehalten werden (Zwei-Stufen-Prüfung). Es ist wichtig, dass der System-Anbieter gemäß den Anweisungen des System-Kunden handelt.

Eine Übermittlung in ein Drittland oder an eine internationale Organisation i.S.v. Art. 44 ff. DS-GVO liegt vor, wenn personenbezogene Daten aus der EU bzw. dem EWR in ein Land oder mehrere Länder außerhalb der EU bzw. des EWR oder an eine internationale Organisation übermittelt werden. Eine Übermittlung i.d.S. liegt auch vor, wenn die personenbezogenen Daten durch Fernzugriff einem Akteur außerhalb der EU bzw. des EWR zugänglich gemacht oder mitgeteilt werden.[55] Eine internationale Organisation ist gemäß Art. 4 Nr. 26 DS-GVO eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Beinhaltet die Auftragsverarbeitung die weisungsgebundene Datenübermittlung an Drittländer oder an internationale Organisationen, verpflichtet Art. 44 DS-GVO zusätzlich zu den Anforderungen an die Auftragsverarbeitung zur Einhaltung der Bedingungen von Kapitel V DS-GVO. Es sollte beachtet werden, dass die Regelung des Art. 49 DS-GVO keine Erlaubnistatbestände für die systematische und regelmäßige Datenübermittlung zwischen Exporteur und Importeur[56] enthält. Systematische und regelmäßige Datenübermittlungen zwischen Exporteur und Importeur müssen daher auf Angemessenheitsbeschlüsse nach Art. 45 Abs. 3 DS-GVO (eine Liste der gültigen Angemessenheitsbeschlüsse findet sich auf der Website der EU-Kommission[57]) oder geeignete Garantien nach Art. 46 Abs. 2 oder 3 DS-GVO gestützt werden, die zwischen dem System-Anbieter und dem System-Kunden nach Nr. 1.4 festgelegt worden sind. Datenübermittlungen auf Grundlage von Art. 49 DS-GVO dürfen allenfalls in sehr restriktiven Ausnahmefällen erfolgen.

Art. 46 Abs. 2 und 3 DS-GVO nennt verschiedene Übermittlungsinstrumente, die geeignete Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus im Drittland darstellen können und die für alle Drittländer einheitlich angewendet werden können. Wegen der besonderen rechtlichen und/oder praktischen Gegebenheiten in einem Drittland, in das personenbezogene Daten übermittelt werden sollen, kann es allerdings erforderlich sein, dass der System-Anbieter diese Übermittlungsinstrumente um zusätzliche organisatorische, technische und/oder vertragliche Maßnahmen ergänzt, um ein angemessenes Datenschutzniveau sicherzustellen, das im Wesentlichen dem der DS-GVO entspricht.

Es ist zu beachten, dass die Verwendung der EU-Standardvertragsklauseln vom Juni 2021 (EU-SVK) allein kein angemessenes Datenschutzniveau gewährleitet. Vielmehr muss der System-Anbieter auch bei diesem Übermittlungsinstrument, ggf. mit dem Empfänger gemeinsam, prüfen, ob Rechtslage und Praxis des Drittlands die Effektivität der EU-SVK beeinträchtigen. Diese Prüfung ist auch bei der Verwendung der anderen geeigneten Garantien nach Art. 46 Abs. 2 und 3 DS-GVO durchzuführen. Liegt eine Beeinträchtigung vor, darf die Datenübermittlung nicht stattfinden oder es müssen zusätzliche Maßnahmen ergriffen werden, um die identifizierten Lücken zu schließen und ein angemessenes Datenschutzniveau im Drittland sicherzustellen.

Dem Recht eines Drittlands, das zu einer Offenlegung von personenbezogenen Daten an staatliche Stellen des jeweiligen Drittlands verpflichtet, können System-Anbieter unterliegen, wenn sie Daten ganz oder teilweise im jeweiligen Drittland verarbeiten, aber auch wenn sie, z. B. als europäisches Tochterunternehmen eines Mutterkonzerns aus einem Drittland, personenbezogene Daten ausschließlich auf Servern in der EU oder im EWR verarbeiten. Auch in diesem Fall kann der System-Anbieter nach dem Recht von Drittländern verpflichtet sein, personenbezogene Daten, die sich auf Servern in der EU oder im EWR befinden, gegenüber staatlichen Stellen des betreffenden Drittlands offenzulegen, wenn er durch gerichtliches Urteil oder Entscheidungen von Verwaltungsbehörden dazu verpflichtet wird. Dies ist z. B. für europäische Tochterunternehmen von US-Mutterkonzernen im Rahmen des CLOUD Acts der Fall. Solche rechtlichen Offenlegungspflichten nach dem Recht von Drittländern stehen in Konflikt mit Art. 48 DS-GVO. Dieser verpflichtet Verantwortliche und Auftragsverarbeiter dazu, jeglichen Urteilen von Gerichten von Drittländern und jeglichen Entscheidungen von Verwaltungsbehörden von Drittländern, mit denen eine Offenle-

[55] S. EDSA, Leitlinien 5/2021, S. 9.
[56] Datenexporteur ist/sind die natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) ("Stelle(n)"), die die personenbezogenen Daten in ein Drittland übermittelt/übermitteln. Die Stelle(n) in einem Drittland, die die personenbezogenen Daten vom Datenexporteur direkt oder indirekt über eine andere Stelle erhält/erhalten, ist/sind der Datenimporteur, s. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.
[57] Website der Kommission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=de; s.a. Website des HBDI, https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission.

gung personenbezogener Daten verlangt wird, nur Folge zu leisten, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Der Auftragsverarbeiter hat die Bewertung von Recht und Praxis des Drittlandes dem Verantwortlichen bereitzustellen, damit dieser überprüfen kann, ob die von dem Auftragsverarbeiter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in das Drittland übermittelten personenbezogenen Daten gewährleisten.

Es versteht sich von selbst, dass weiterhin die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung im Hinblick auf Datenübermittlungen eingehalten werden muss, s. insbesondere Nr. 1.4.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 5/2021 zum Zusammenspiel zwischen Art. 3 und Kapitel V der Datenschutz-Grundverordnung
- DSK, Kurzpapier Nr. 4 Datenübermittlung in Drittländer
- ISO/IEC 27701:2025 Ziff. B.2.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten

Der EDSA hat in seinen Empfehlungen eine sechsschrittige Prüfung veröffentlicht, die angibt, wie der System-Anbieter vorgehen sollte, um festzustellen, ob die Instrumente nach Art. 46 Abs. 2 oder 3 DS-GVO hinreichend sind, um ein angemessenes Datenschutzniveau für die Datenübermittlung in das betreffende Drittland sicherzustellen, oder ob zusätzliche Maßnahmen ergriffen werden müssen, um ein angemessenes Datenschutzniveau sicherzustellen.[58]

Besonderes Augenmerk sollte auf den 3. und 4. Schritt der Prüfung gelegt werden: Im 3. Schritt der Prüfung ist zu überprüfen, ob Rechtslage und Rechtspraxis im Drittland die Wirksamkeit der angemessenen Garantien nach Art. 46 Abs. 2 oder 3 DS-GVO bei der konkreten Datenübermittlung beeinträchtigen. Sollte dies der Fall sein, sollte im 4. Schritt der Prüfung geprüft werden, ob zusätzliche Maßnahmen effektiv ergriffen werden können, um ein angemessenes Datenschutzniveau sicherzustellen. Im Rahmen der Prüfung des 3. Schritts sollten zunächst die Rechtsvorschriften des betreffenden Drittlands beleuchtet werden.

Für die einzelnen Übermittlungsinstrumente, die in Art. 46 Abs. 2 DS-GVO enthalten sind, wird auf folgende Empfehlungen und Leitlinien verwiesen:

- Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates
- EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten
- EDSA, Leitlinien 4/2021 Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e DS-GVO)
- EDSA, Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO)
- EDSA, Leitlinie 7/2022 Genehmigter Zertifizierungsmechanismus nach Art. 42 DS-GVO (Art. 46 Abs. 2 lit. f DS-GVO)

Rechtsvorschriften, die gesetzliche Befugnisse für staatliche Stellen auf Zugang zu personenbezogenen Daten implizit oder explizit regeln, sind für die Bewertung von Rechtslage und Rechtspraxis zu berücksichtigen. Speziell für die USA betrifft dies (exemplarisch und nicht abschließend) den Foreign Intelligence Surveillance Act (FISA), den Clarifying Lawful Overseas Use of Data Act (CLOUD Act) und die Executive Order 12333 (United States intelligence activities).

[58] EDSA, Empfehlungen 01/2020.

- System-Anbieter mit Sitz in den USA unterliegen dem US-amerikanischen FISA, der es staatlichen US-Stellen in Sec. 702 FISA gestattet, auf durch US-Unternehmen („electronic communication service providers“) verarbeitete Daten von Nicht-US Bürgern, die in den USA gespeichert sind, Zugriff zu nehmen. Für diese Rechtsnorm hat der EuGH festgestellt, dass die Zugangsbefugnisse auf personenbezogene Daten nicht auf das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß beschränkt sind, so dass die Verwendung von geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DS-GVO für eine Datenübermittlung allein nicht zu einem gleichwertigen Schutzniveau in den USA führt.

- Auch der CLOUD Act ermöglicht es staatlichen US-Stellen, von US-Unternehmen den Zugriff auf Daten von Nicht-US-Bürgern zu erzwingen, wenn die Unternehmen in der Lage sind, diesen Zugang zu ermöglichen, auch wenn diese auf europäischen Servern liegen. Dies ist bei einem System-Anbieter der Fall, wenn dieser ein europäisches Tochterunternehmen eines US-Mutterkonzerns ist. Diese Zugriffsrechte gehen über das Maß hinaus, das in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist. Schließlich hat das dem CLOUD Act unterliegende Unternehmen bei personenbezogenen Daten von Europäern kaum effektive Möglichkeiten, die Anordnung der staatlichen US-Stelle gerichtlich überprüfen zu lassen, da diese Möglichkeit nur gegeben ist, wenn der Empfänger durch die Offenlegung zur Verletzung von Gesetzen qualifizierter ausländischer Regierungen verleitet würde. Weder Deutschland noch die EU haben ein Exekutiv-Abkommen mit den USA abgeschlossen, das sie zu einer solchen qualifizierten ausländischen Regierung machen würde. Ein unabhängiger Aufsichtsmechanismus als Säule der wesentlichen europäischen Garantien liegt somit nicht vor, sodass kein gleichwertiges Datenschutzniveau angenommen werden kann. Zudem steht eine solche Offenlegung in Widerspruch zu Art. 48 DS-GVO, da zwischen Deutschland/der EU und den USA kein Rechtshilfeabkommen besteht und personenbezogene Daten daher nicht an die staatlichen US-Stellen gegeben werden dürfen.

- Die Executive Order 12333 zielt auf die geheimdienstliche Informationsausstattung des Präsidenten, des National Security Council und des Homeland Security Council. Eine effektive Beschränkung der Maßnahmen zur Informationsgewinnung ausschließlich auf US-Bürger ist hierin nicht vorgesehen. Auch diese Regelung verhindert ein gleichwertiges Datenschutzniveau.

Rechtsvorschriften sollten jedoch nicht als einzige Quelle genutzt werden, da sie formal ein gleichwertiges Datenschutzniveau suggerieren können, welches in der Rechtspraxis jedoch nicht gewährleistet wird. Neben den Rechtsvorschriften selbst, sollten daher, sofern für das betreffende Drittland vorhanden, auch folgende Quellen berücksichtigt werden:

- die Rechtsprechung des EuGH wie z. B. das Schrems II-Urteil für die USA oder die Rechtsprechung des EGMR wie z. B. das Faktenblatt zur Massenüberwachung (EGMR, factsheet – mass surveillance);

- Angemessenheitsbeschlüsse für das Drittland, wenn die Datenübermittlung auf einem anderen Übermittlungsinstrument beruht;

- Resolutionen und Berichte zwischenstaatlicher Organisationen wie bspw. des Europarats oder regionaler Organisationen wie z. B. die Länderberichte der Interamerikanischen Kommission für Menschenrechte oder Organisationen der Vereinten Nationen wie z. B. des Menschenrechtsrats oder der Menschenrechtskommission der Vereinten Nationen;

- Berichte und Analysen von zuständigen Regulierungsnetzwerken wie z. B. der Global Privacy Assembly (GPA);

- Nationale Rechtsprechung oder Entscheidungen unabhängiger Justiz- oder Verwaltungsbehörden, die für Datenschutz und den Schutz der Privatsphäre in Drittländern zuständig sind;

- Berichte unabhängiger Kontrollorgane oder parlamentarischer Gremien;

- Berichte über praktische Erfahrungen mit früheren Fällen von Offenlegungsersuchen von staatlichen Stellen oder dem Ausbleiben solcher Ersuchen von Einrichtungen, die in der gleichen Branche wie der Empfänger tätig sind;

- „Warrant Canary"-Erklärungen anderer Unternehmen, die Daten in der gleichen Branche wie der Empfänger verarbeiten;
- Berichte, die von Handelskammern, Wirtschafts-, Berufs- und Handelsverbänden, staatlichen diplomatischen Vertretungen, Handels- und Investitionsagenturen des Exporteurs oder anderen Drittländern, die in das Drittland, in das die Datenübermittlung erfolgen soll, exportieren, erstellt oder in Auftrag gegeben wurden;
- Berichte von akademischen Einrichtungen und Organisationen der Zivilgesellschaft (z. B. NGOs).

Die praktischen Erfahrungen des Empfängers dürfen in die Gesamtbewertung über das Datenschutzniveau des Drittlands einfließen, sie darf sich jedoch nicht ausschließlich darauf stützen. Die praktischen Erfahrungen sollten nach Möglichkeit untermauert werden, z. B. durch Erfahrungsberichte anderer Unternehmen, die in der gleichen Branche arbeiten oder z. B. durch investigative Artikel namhafter Zeitungen oder wissenschaftliche Aufsätze in Fachzeitschriften, die sich mit den spezifischen Rechtsvorschriften und der tatsächlichen Rechtspraxis befassen. Hat der Empfänger bisher keine Offenlegungsersuchen erhalten, sollte daraus nicht der Schluss gezogen werden, dass diese auch für die Zukunft ausgeschlossen sind. Alle herangezogenen Quellen zur Beurteilung von Rechtslage und Rechtspraxis sollten sorgfältig dokumentiert werden. Rechtsvorschriften sollten mit vollständigem Namen der Rechtsvorschrift und den einschlägigen Paragrafen dokumentiert werden. In die Bewertung einbezogene Berichte, Urteile etc. sollten ebenfalls klar benannt werden. Insofern empfiehlt sich ein aktuell zu haltendes Fundstellenmanagement.

Bei der Beurteilung von Rechtslage und Rechtspraxis im Drittland ist es wichtig zu prüfen, ob die konkrete Datenübermittlung in den Anwendungsbereich von Gesetzen fällt, die staatlichen Stellen des Drittlandes Befugnisse zum Zugang auf personenbezogene Daten einräumen, die über das hinausgehen, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Für diese Bewertung können die „wesentlichen europäischen Garantien" aus den „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen" des EDSA als Bewertungsmaßstab herangezogen werden.

Die nachfolgenden Ausführungen zu den wesentlichen europäischen Garantien stellen eine verkürzte Zusammenfassung der „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen" des EDSA dar, um dem System-Anbieter eine erste Orientierung für die Bewertung der Rechtsvorschriften und Rechtspraxis im Drittland zu geben. Die vier wesentlichen europäischen Garantien sollten als Hauptvoraussetzungen verstanden werden, die nicht unabhängig voneinander, sondern in ihrer Gesamtheit geprüft werden sollten, wenn es darum geht, zu beurteilen, ob Zugangsmaßnahmen auf personenbezogene Daten von staatlichen Stellen von Drittländern auf das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß beschränkt sind oder nicht. Für weitere Hinweise für die Bewertung wird auf die Empfehlungen 02/2020 des EDSA verwiesen.

Die vier wesentlichen europäischen Garantien sind:

1. Klare, präzise und zugängliche Vorschriften für die Datenverarbeitung

Gesetzliche Vorschriften für den Zugang von staatlichen Stellen zu personenbezogenen Daten müssen klare, präzise und öffentlich zugängliche Regeln für die Anwendung der betreffenden Zugangsmaßnahmen und Mindestanforderungen an diese vorsehen. Dies beinhaltet auch, dass die Rechtsvorschrift regeln muss, unter welchen Umständen und Bedingungen eine Zugangsmaßnahme durch die staatliche Stelle angewendet werden darf und in welchem Umfang die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten der betroffenen Person eingeschränkt werden dürfen. Zudem muss die gesetzliche Vorschrift Folgendes definieren: Personengruppen, die von Zugangsmaßnahmen betroffenen sein können, zeitliche Begrenzungen der Zugangsmaßnahmen, Verfahren für die Auswertung, Verwendung und Speicherung der gewonnenen Daten und zu treffende Vorsichtsmaßnahmen für die Übermittlung der Daten an andere Parteien. Weiterhin muss die gesetzliche Vorschrift rechtsverbindlich sein und den betroffenen Personen Rechte gegenüber der staatlichen Stelle verleihen, die sie gerichtlich geltend machen und durchsetzen können. Liegen keine öffentlich zugänglichen Vorschriften vor, die den Zugang von staatlichen Stellen auf personenbezogene Daten regeln oder werden den betroffenen Personen keine Rechte gegenüber der Behörde eingeräumt, kann kein gleichwertiges Schutzniveau für das Drittland angenommen werden.

2. Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele

Nach Art. 52 Abs. 1 Satz 1 GRCh muss jede Einschränkung der in der Charta anerkannten Rechte den Wesensgehalt dieser Rechte achten, weshalb Einschränkungen durch Zugangsmaßnahmen nur vorgenommen werden dürfen, wenn sie unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und sie in der EU anerkannten Zielsetzungen des Gemeinwohls dienen oder dem Schutz von Rechten und Freiheiten anderer entsprechen. Um zu beurteilen, ob eine Einschränkung verhältnismäßig ist, kommt es zum einen auf die Schwere des Eingriffs an, der mit der Einschränkung verbunden ist, und zum anderen, ob die mit der Einschränkung verfolgte Zielsetzung des Gemeinwohls der Schwere des Eingriffs angemessen ist. So ist z. B. ein Zugang durch staatliche Stellen auf den Standort eines Mobiltelefons einer betroffenen Person in Echtzeit ein schwerer Eingriff, weil er der staatlichen Stelle ermöglicht, jederzeit die Bewegungen der betroffenen Person zu verfolgen. Er könnte aber angemessen sein, wenn er etwa auf die Verhinderung unmittelbar bevorstehender, schwerwiegender Terrorismusakte oder auf die Suche nach Verletzten oder Vermissten abzielt. Die Einschränkung eines Rechts muss auf das absolut Notwendige beschränkt sein, was voraussetzt, dass für die Zugangsmaßnahmen durch gesetzliche Vorschriften präzise geregelt sein muss, wann, unter welchen Umständen und Voraussetzungen die Zugangsmaßnahmen eingesetzt werden dürfen und welche Mindesterfordernisse die staatliche Stelle hierbei einhalten muss. Gesetzliche Vorschriften, die Eingriffe i.S.v. Zugangsmaßnahmen auf personenbezogene Daten durch staatliche Stellen erlauben, ohne hierfür Einschränkungen vorzusehen, genügen den Anforderungen an ein gleichwertiges Datenschutzniveau nicht, da jede gesetzliche Vorschrift für einen Eingriff den Umfang der Einschränkung der jeweiligen Rechte definieren muss. Weiterhin ist der Grundsatz der Erforderlichkeit nicht eingehalten, wenn gesetzliche Vorschriften für Zugangsmaßnahmen den Wesensgehalt von Rechten missachten. Dies ist z. B. für Art. 7 GRCh der Fall, wenn staatliche Stellen durch gesetzliche Vorschriften befugt sind, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, ohne dass der Eingriff beschränkt wird, die mit dem Eingriff verfolgten Ziele benannt sind und objektive Kriterien für den Einsatz der Zugangsmaßnahme definiert werden.

3. Unabhängiger Aufsichtsmechanismus

Weiterhin muss im Drittland für jeden Eingriff in die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten eine wirksame, unabhängige und unparteiische Aufsicht durch einen Richter oder eine andere unabhängige Stelle etabliert sein. Der Aufsichtsmechanismus muss einerseits sicherstellen, dass manche Zugangsmaßnahmen durch staatliche Stellen von der vorherigen Genehmigung eines Richters oder einer unabhängigen Stelle abhängig gemacht werden und diese Genehmigung oder Ablehnung bindend ist. Andererseits muss der Aufsichtsmechanismus über alle Befugnisse verfügen, um Kontrollen wirksam durchführen und etwaiges missbräuchliches Handeln durch staatliche Stellen feststellen zu können. Dies erfordert etwa Zugang zu sämtlichen relevanten Schriftstücken, u.a. auch zu Verschlusssachen. Die Unabhängigkeit des Aufsichtsmechanismus setzt zudem voraus, dass er über eine hinreichende Unabhängigkeit von der Exekutive verfügt. Ebenso wichtig ist aber auch, dass die Tätigkeit der die Aufsicht ausübenden Stelle selbst einer öffentlichen Kontrolle unterliegt, d.h. dass auch ihr Ergebnis entsprechend unabhängig und unparteiisch überprüfbar ist.

4. Wirksame Rechtsbehelfe

Nach Art. 47 Abs. 1 GRCh hat jede Person, die der Ansicht ist, dass ihre durch EU-Recht garantierten Rechte oder Freiheiten verletzt worden sind, das Recht, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Dies erfordert etwa bei Eingriffen, die im Verborgenen in die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten stattfinden, auch die nachträgliche Benachrichtigung der betroffenen Person hierüber. Eine gleichwertige Garantie muss auch im Drittland gegeben sein, was bedeutet, dass die betroffene Person im Drittland die Möglichkeit haben muss, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht oder Organ einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten oder ihre Berichtigung oder Löschung zu erwirken. Das Gericht oder Organ muss insbesondere gegenüber der Exekutive unabhängig sein und ermächtigt sein, verbindliche Entscheidungen gegen die betreffenden staatlichen Stellen zu treffen.

Führt die Beurteilung von Rechtslage und Rechtspraxis im Drittland zum Ergebnis, dass die Instrumente aus Art. 46 Abs. 2 und 3 DS-GVO nicht ausreichend sind, um ein angemessenes Datenschutzniveau sicherzustellen, darf die Datenübermittlung nicht ohne zusätzliche Maßnahmen stattfinden.

Gemäß Art. 28 Abs. 3 lit. a DS-GVO muss der Verantwortliche von dem Auftragsverarbeiter die Beurteilung erhalten, die er im Hinblick auf die Rechtsvorschriften und Praktiken des Drittlandes vorgenommen hat, um zu prüfen, ob die von dem Auftragsverarbeiter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau hinsichtlich der in das Drittland übermittelten personenbezogenen Daten gewährleisten. Es versteht sich von selbst, dass der Auftragsverarbeiter bei Datenübermittlungen nach wie vor an die Weisungen des Verantwortlichen gebunden ist, wie sie in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt sind (Nr. 1.4), weshalb eine Übermittlung nur auf Weisung des Verantwortlichen erfolgen kann.

Soll die Datenübermittlung dennoch stattfinden, sollte der System-Anbieter ggf. mit dem Empfänger zusammen im 4. Schritt der Prüfung überprüfen, ob durch zusätzliche Maßnahmen ein angemessenes Datenschutzniveau im Drittland sichergestellt werden kann. Grundsätzlich können zusätzliche Maßnahmen vertraglicher, organisatorischer oder technischer Art sein. Um ein gleichwertiges Schutzniveau im Drittland zu erreichen, kann eine Kombination mehrerer Maßnahmen sinnvoll sein.

Sinnvoll ist z. B. eine vertragliche Zusicherung durch den Empfänger, dass er nicht absichtlich Hintertüren, sonstige technischen Möglichkeiten oder Geschäftsprozesse etabliert hat, die staatlichen Stellen Zugang zum System und zu personenbezogenen Daten verschaffen oder diesen erleichtern und dass er nach dem nationalen Recht des Drittlands auch nicht verpflichtet ist, Hintertüren zu etablieren, staatlichen Stellen Zugang zu personenbezogenen Daten zu verschaffen und Verschlüsselungsschlüssel zu besitzen oder herauszugeben. Sinnvoll ist es auch, den Empfänger zu verpflichten, den Exporteur umgehend zu informieren, wenn Änderungen im nationalen Recht oder in der Rechtspraxis dazu führen, dass die genannten Zusicherungen nicht mehr eingehalten werden können, so dass der Exporteur den Vertrag kurzfristig kündigen und die Datenübermittlung beenden kann. Zu beachten ist jedoch, dass solche Zusicherungen des Empfängers nach dem nationalen Recht des Drittlands untersagt sein können.

Unterliegt ein Empfänger nationalen Gesetzen, die einem der DS-GVO gleichwertigen Schutzniveau im jeweiligen Drittland entgegenstehen, werden vertragliche und organisatorische Maßnahmen allein i.d.R. nicht ausreichen, um einen Zugang auf personenbezogene Daten durch staatliche Stellen des Drittlands zu verhindern, so dass technische Maßnahmen ergriffen werden sollten.

Die folgenden drei Use Cases sollen eine Hilfestellung bieten, wann zusätzliche technische Maßnahmen zu einem gleichwertigen Datenschutzniveau beitragen können und wann nicht:

1. Use Case: Datenübermittlung an einen Empfänger z. B. für Backup-Zwecke, bei der der Empfänger keinen Zugriff auf die personenbezogenen Daten im Klartext benötigt bzw. in dem der Empfänger einen Zugriff auf die personenbezogenen Daten im Klartext nicht anfragt oder nutzt. Die Verschlüsselung vor der Datenübermittlung stellt eine wirksame zusätzliche technische Maßnahme dar, wenn

    a. eine starke Verschlüsselung gewählt wird und die Identität des Empfängers geprüft wird;

    b. der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, Betriebsart) dem Stand der Technik entsprechen und – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen die von den Behörden im Drittland durchgeführte Kryptoanalyse bieten;

    c. die Verschlüsselungsstärke den Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist;

    d. der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert ist, deren Konformität mit der Spezifikation des ausgewählten Algorithmus bestätigt wurde;

    e. die Schlüssel beim Exporteur zuverlässig verwaltet (erzeugt, angewandt, gespeichert, falls relevant, mit der Identität des vorgesehenen Empfängers verknüpft sowie widerrufen) werden und

    f. die Kontrolle über die Schlüssel allein beim Exporteur oder bei anderen mit dieser Aufgabe betrauten Stellen im EWR oder in einem Drittland mit Angemessenheitsbeschluss liegt.

Die ISO/IEC 11770-2 enthält weitere Informationen zur Schlüsselverwaltung. Weiterhin bieten die Technischen Reporte des BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen"; BSI TR-02102-3 „Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2)"; und BSI TR-02102-4 „Kryptographische Verfahren: Verwendung von Secure Shell (SSH)" weitere hilfreiche Hinweise für die Verschlüsselung, so dass auf diese hingewiesen wird.

Zum Stand der Technik bei Verschlüsselungsverfahren und anderen TOM kann auf die „Handreichung zum Stand der Technik" von TeleTrust in der aktuellen Fassung verwiesen werden.

2. Use Case: Verarbeitung pseudonymisierter Daten durch den Empfänger im Drittland. Die Pseudonymisierung der Daten durch den Exporteur vor der Datenübermittlung an den Empfänger stellt eine wirksame zusätzliche technische Maßnahme dar, wenn

    a. der Exporteur die personenbezogenen Daten in solcher Weise übermittelt, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren;

    b. die zusätzlichen Informationen allein vom Exporteur vorgehalten werden, und zwar separat in einem Mitgliedstaat oder in einem Drittland, bei einer vom Exporteur betrauten Stelle im EWR oder in einer Rechtsordnung, die ein dem EWR im Wesentlichen gleichwertiges Schutzniveau bietet;

    c. die Offenlegung oder die unerlaubte Verwendung der zusätzlichen Informationen durch geeignete technische und organisatorische Garantien verhindert wird und sichergestellt ist, dass die Kontrolle über den Algorithmus oder den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, allein beim Exporteur liegt, und

    d. der Verantwortliche durch gründliche Analyse der betreffenden Daten, unter Berücksichtigung sämtlicher Informationen, die den staatlichen Stellen im Empfängerland erwartungsgemäß zur Verfügung stehen, festgestellt hat, dass die pseudonymisierten personenbezogenen Daten keiner identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, selbst wenn sie mit derartigen Informationen abgeglichen werden.

    Weiterhin sollten die Ausführungen in den Randnummern 86 bis 89 der Empfehlungen 01/2020 des EDSA beachtet werden.

3. Use Case: Datenübermittlung an einen Empfänger, der aufgrund der Art der Subauftragsverarbeitung Zugang zu unverschlüsselten Daten benötigt: Findet auf den Empfänger das Recht eines Drittlands Anwendung, das staatlichen Stellen Zugang zu personenbezogenen Daten gewährt, das über das Maß hinausgeht, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, reichen technische Maßnahmen wie Transportverschlüsselung während der Übermittlung und die Verschlüsselung von personenbezogenen Daten im Ruhezustand nicht aus, um die Rechte der betroffenen Personen zu schützen. Auch die Kombination der genannten technischen Maßnahmen mit zusätzlichen vertraglichen Maßnahmen, wie z. B. die vertraglich zugesicherte Pflicht des Importeurs zugegangene Offenlegungsersuche von staatlichen Stellen anzufechten und den nationalen Rechtsweg gegen ein Offenlegungsersuchen zu bestreiten, oder die vertragliche Pflicht, den Exporteur über eingegangene Offenlegungsersuche vor der Datenübermittlung an die staatliche Stelle zu informieren, reichen nicht aus, um eine Datenübermittlung in das betreffende Drittland zu legitimieren. Im 3. Use Case muss die Datenübermittlung daher unterlassen werden.

Eine nicht abschließende Aufzählung zusätzlicher vertraglicher, organisatorischer oder technischer Maßnahmen sowie eine Auflistung weiterer Use Cases ist in Anhang 2 der Empfehlungen 01/2020 des EDSA enthalten, auf die hiermit verwiesen wird.

System-Anbieter, die auch dem Recht von Drittländern unterliegen, müssen gemäß Art. 48 DS-GVO die Herausgabeverlangen von staatlichen Stellen von Drittländern bezüglich personenbezo-

gener Daten aus der EU und dem EWR grundsätzlich ablehnen und auf in Kraft befindliche internationale Übereinkünfte wie z. B. Rechtshilfeabkommen verweisen, soweit diese mit dem betreffenden Drittland bestehen.

Wenn der System-Anbieter personenbezogene Daten verarbeitet und nicht nur dem Recht der DS-GVO unterliegt, sondern zugleich dem Recht eines Drittlands, das ihn zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des betreffenden Drittlands verpflichtet, sind zum Schutz der europäischen Grundrechte und Grundfreiheiten der betroffenen Personen zusätzliche Maßnahmen zu ergreifen, um die personenbezogenen Daten vor einer Offenlegung gegenüber den staatlichen Stellen des Drittlands zu schützen. Eine denkbare Lösung ist z. B. ein Treuhandmodell, bei dem die Daten im Besitz und in der Herrschaft eines Unternehmens verbleiben, das ausschließlich europäischem Recht unterliegt. Bezüglich anderer denkbarer zusätzlicher Maßnahmen, die zum Schutz der europäischen Grundrechte und Grundfreiheiten ergriffen werden sollten, können in manchen Fällen auch die zusätzlichen Maßnahmen aus Anhang 2 der Empfehlungen 01/2020 des EDSA hilfreich sein, weshalb auf diesen verwiesen wird. Auch hier sollte beachtet werden, dass zusätzliche vertragliche oder organisatorische Maßnahmen im Regelfall nicht ausreichen werden, um die personenbezogenen Daten vor einer Offenlegung gegenüber staatlichen Stellen von Drittländern zu schützen, so dass sie mit technischen Maßnahmen kombiniert werden sollten.

Nr. 14.2 - Vertreterbenennung
(Art. 27 i.V.m. Art. 3 Abs. 2 DS-GVO)

Kriterium

1) System-Anbieter ohne Niederlassung in der EU oder im EWR, für die dennoch gemäß Art. 3 Abs. 2 DS-GVO die DS-GVO gilt, benennen schriftlich einen Vertreter in der EU oder im EWR. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die betroffenen Personen befinden, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird.

2) Der System-Anbieter beauftragt den Vertreter als Ansprechpartner für sämtliche Fragen im Zusammenhang mit der Datenverarbeitung zur Gewährleistung der Einhaltung der DS-GVO und erteilt dem Vertreter die notwendigen Vollmachten, damit dieser im Namen des System-Anbieters und an dessen Stelle tätig werden kann, um die Pflichten der DS-GVO zu erfüllen.

Erläuterung

Ein Vertreter i.d.S. ist gemäß Art. 4 Nr. 17 DS-GVO eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Art. 27 DS-GVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt.

Umsetzungshinweis

Der System-Anbieter kann bei der Beauftragung entscheiden, ob der Vertreter ergänzend zu ihm oder allein als Ansprechpartner auftreten soll; dies ist entsprechend im Außenverhältnis zu kommunizieren. Bietet der System-Anbieter ohne Niederlassung in der EU oder im EWR seine Dienstleistung in mehreren Mitgliedstaaten an, muss er nicht in jedem Mitgliedstaat einen Vertreter benennen, vielmehr ist auch ein Vertreter in einem Mitgliedstaat mit Zuständigkeit für mehrere Mitgliedstaaten zulässig, solange sich in diesem betroffene Personen befinden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2022 Ziff. 5.2 Informationssicherheitsrollen und -verantwortlichkeiten
- ISO/IEC 27701:2025 Ziff. B.2.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.3.4 Informationssicherheitsrollen und -verantwortlichkeiten

Kapitel V: Ergänzende Anforderungen an spezifische Arten von schulischen Informationssystemen

Nr. 15 – Videokonferenzsysteme und andere digitale Kommunikationssysteme

Kriterium

1) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass die Systeme nur die Daten verarbeiten, die für ihre Bereitstellung zwingend erforderlich sind. Er hat die zum Schutz der Rechte der betroffenen Personen, zur Gewährleistung des Kinder- und Jugendschutzes, zur Verhinderung der missbräuchlichen Nutzung sowie zur Wahrung der Vertraulichkeit des Fern-, Wechsel- oder Hybridunterrichts erforderlichen TOM zu ergreifen.

2) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass es für den System-Kunden bzw. dessen Mitarbeitende möglich ist, eine Bild- oder Tonkonferenz sowie vergleichbare aufnahmebasierte Kommunikationen jederzeit beenden zu können sowie einzelne missbrauchsanfällige Funktionalitäten abschalten zu können, so dass sie für die System-Nutzer nicht mehr nutzbar sind.[59] Die Inanspruchnahme missbrauchsanfälliger Funktionalitäten muss protokollierbar sein.

3) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen muss allen System-Nutzern die Möglichkeit geben, ihre Aufnahmegeräte selbstbestimmt auszuschalten. Die Aufnahmegeräte müssen beim Beitritt eines System-Nutzers standardmäßig ausgeschaltet sein. Aufnahmegeräte dürfen nicht entgegen dem Willen der System-Nutzer einschaltbar sein. Die Möglichkeit der System-Nutzer, ihre Aufnahmegeräte einzuschalten, muss abschaltbar sein.

4) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass Bild- und Tonaufzeichnungen, die über eine im System integrierte Funktion vorgenommen und beim System-Anbieter gespeichert werden, jederzeit vom System-Kunden oder auf dessen Weisung gelöscht werden können. Wenn vom System-Kunden gefordert, muss der System-Anbieter durch TOM die Anfertigung von Bild- und Tonaufzeichnung durch im System integrierte Funktionen vollständig ausschließen können. Der System-Anbieter hat den System-Nutzer mindestens bei erstmaliger Anfertigung von Bild- und Tonaufzeichnung darauf hinzuweisen, dass die Aufzeichnung ggf. nur bei der Verwendung dienstlicher Geräte erlaubt ist.

5) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen macht für die System-Nutzer von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen in einfacher und leicht verständlicher Weise erkennbar, welche personenbezogenen Daten zu welchen Zwecken im Rahmen des Systems verarbeitet werden. Es muss insbesondere erkennbar sein, ob Bild- und Tonaufzeichnungen stattfinden. Jegliche gesetzlich vorgeschriebenen und freiwilligen Informationshinweise müssen in für Minderjährige leicht verständlicher Form angeboten werden. Diese Informationen sind an prominenter Stelle im Rahmen der Systemnutzung zu platzieren.

6) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen sieht TOM vor, die eine Zugriffskontrolle nach dem Stand der Technik ermöglichen. Diese TOM müssen ein Rollenverteilungskonzept oder ein gleichwertiges Zugriffskonzept enthalten. Die Zugriffskontrolle muss den System-Kunden dazu befähigen, den verschiedenen System-Nutzern durch den System-Kunden definierte oder durch den System-Anbieter vordefinierte Zugriffsrechte auf verschiedene Funktionen des Videokonferenzsystems oder der anderen digitalen Kommunikationssysteme zu geben. Im Rahmen

[59] Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann. Funktionalitäten, die genutzt werden können, um den Unterricht zu stören (z. B. durch das ständige Betreten und Verlassen oder das virtuelle Heben der Hand), sollten ebenfalls abschaltbar sein, werden von diesem Kriterium aber nur erfasst, wenn mit ihnen eine Verarbeitung personenbezogener Daten einhergeht. S. DSK, Orientierungshilfe Videokonferenzsysteme, S. 19.

von Maßnahmen, die eine Rollenverteilung umfassen, muss die Nutzung eines Gastprofils möglich sein, sofern ein Gastzugang für die Erfüllung des Bildungs- und Erziehungsauftrages des System-Kunden notwendig ist.

7) Der System-Anbieter stellt durch TOM sicher, dass die Nutzung des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme nur authentifizierten Nutzern möglich ist. Diese müssen sich mithilfe eines Nutzernamens und eines nach initialer Authentifizierung durch den Nutzer veränderten Passworts anmelden. Authentifizierungsverfahren, die ein vergleichbares oder höheres Schutzniveau gewährleisten, sind ebenfalls zulässig. Für Gastzugänge ist eine Authentifizierung nicht erforderlich. Der Missbrauch eines Gastzuganges ist durch eine restriktive Zuweisung von Rechten oder vergleichbare TOM hinreichend sicher auszuschließen.

8) Sofern ein Videokonferenzsystem oder ein anderes digitales Kommunikationssystem die Möglichkeit der Einsichtnahme in Nutzungsdaten sowie Kommunikationsinhalte beinhaltet, darf dies nur bestimmten Personen möglich sein. Sofern ein Rollenverteilungskonzept i.S.d. Abs. 6 genutzt wird, darf ein Zugriff nur bestimmten Rollen innerhalb des Systems möglich sein. Die Rollen oder anderweitige Zugriffsmöglichkeiten sind so zu definieren, dass die Missbrauchswahrscheinlichkeit der Nutzungsdaten und Kommunikationsinhalte so gering wie möglich ist.

9) Der System-Anbieter stellt durch TOM sicher, dass Videokonferenzsysteme und andere digitale Kommunikationssysteme Verschlüsselungsverfahren nutzen, die dem Stand der Technik entsprechen.

Erläuterung

Im Rahmen schulischer Informationssysteme ist u.a. das besondere Verhältnis zwischen Schule, Lehrkräften, Betreuungspersonal und Schülerinnen und Schülern, welches durch Obhutsbeziehungen und Subordination gekennzeichnet ist, zu berücksichtigen. Dazu gehört auch die eventuell verminderte Urteilsfähigkeit von minderjährigen Personen, die dazu führt, dass sie sich der Risiken, Folgen und Garantien sowie ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise nicht bewusst sind. Daher muss sichergestellt werden, dass bei der Verwendung von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen missbrauchsanfällige Funktionalitäten unterbunden werden können und dieser Vorgang protokolliert werden kann.

Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann.[60] Funktionalitäten, die genutzt werden können, um den Unterricht zu stören (z. B. durch das ständige Betreten und Verlassen oder das virtuelle Heben der Hand), sollten ebenfalls abschaltbar sein, werden von diesem Kriterium aber nur erfasst, wenn mit ihnen eine Verarbeitung personenbezogener Daten einhergeht.

Im Sinne der datenschutzfreundlichen Voreinstellungen müssen Videokonferenzsysteme und andere digitale Kommunikationssysteme so gestaltet sein, dass sie zu Beginn der Nutzung, bevor der System-Nutzer aktiv Einstellungen vornehmen kann, so wenig personenbezogene Daten verarbeiten wie möglich. Daher müssen die Aufnahmegeräte grundsätzlich deaktiviert sein und in der Folge von den System-Nutzern jederzeit autonom ausschaltbar sein.

Da es sich regelmäßig um Kinder und Jugendliche handelt, muss auch die Art der Information über Videokonferenzsysteme und andere digitale Kommunikationssysteme der verminderten Urteilsfähigkeit von Minderjährigen angepasst werden. Daher hat jegliche Information über die Verarbeitung personenbezogener Daten in einfacher und leicht verständlicher Sprache zu erfolgen (s. Art. 12 Abs. 1 Satz 1, 2. Hs. DS-GVO). Zudem ist diese Information so zu platzieren, dass sie vor der Datenverarbeitung und für die Kinder und Jugendlichen leicht erkennbar wahrgenommen werden kann. Die Transparenz sollte insbesondere hinsichtlich der Aufzeichnung der Video- und Tonkonferenzen gewährleistet werden. Eine Aufzeichnung über das System kann zulässig sein, wenn ein legitimer Zweck verfolgt wird (z. B. die Aufzeichnung eines Vortrags zur gemeinsamen Analyse) und diese Aufzeichnung für alle Teilnehmenden der Konferenz deutlich erkennbar ist. Eine solche Erkennbarkeit fehlt regelmäßig bei der Aufnahme durch Drittsysteme (z. B. Bildschirmaufzeichnung). Eine Aufzeichnung durch Drittsysteme sollte – soweit technisch für den System-Anbieter möglich – ausgeschlossen werden (z. B. durch eine Screenshot-Sperre innerhalb des Systems).

[60] S. DSK, Orientierungshilfe Videokonferenzsysteme, S. 19.

Landesgesetzliche Regelungen

In einigen Bundesländern finden sich spezifische Vorschriften zu Videokonferenzsystemen und anderen digitalen Kommunikationssystemen, auf die im Folgenden hingewiesen wird:

- Baden-Württemberg: § 115 Abs. 3a, § 115b Abs. 6-8 SchulG BW.
- Bayern: Art. 30 Abs. 2 BayEUG i.V.m. § 19 Abs. 4 u. 5 BaySchO; Anlage 2 Abschnitt 4 und 7 BaySchO wonach nur die dort aufgezählten Daten im Rahmen der Systemnutzung verarbeitet werden dürfen.
- Berlin: § 4 und § 5 DigLLV Berlin.
- Brandenburg: Es sind keine relevanten spezifischen Regelungen ersichtlich.
- Hamburg: § 98c HmbSG insbesondere § 98c Abs. 3 und 4 HmbSG.
- Hessen: § 83b SchulG-HE; § 18 SchDSV-HE.
- Nordrhein-Westfalen: §§ 120 Abs. 5, 121 Abs. 1 i.V.m § 8 Abs. 2 SchulG NRW.
- Saarland: § 13 SchulwDSV SL zur Einrichtung von Videokonferenzsystemen.
- Schleswig-Holstein: § 4a SchulG SH und § 11 Abs. 4 SchulDSVO SH (digitale Lehr- und Lernformen).
- Thüringen: § 57 Abs. 1 i.V.m. § 45a ThürSchulG (digitale Lehr- und Lernmittel einschließlich Präsenzunterricht).

Umsetzungshinweis

Die Informationen über die Art der personenbezogenen Daten, die im Rahmen der Systembereitstellung verarbeitet werden und die Zwecke der Verarbeitung, sowie andere gesetzlich vorgeschriebene Informationspflichten, die sich sowohl an den Verantwortlichen als auch an den Auftragsverarbeiter richten, sollten vor einer Erstverarbeitung oder Erstverwendung des Systems dargestellt werden.

Hinweise und Informationen nach Abs. 4 und 5 (d.h. Hinweis zur Verwendung dienstlicher Geräte bzw. Anfertigung von Bild- und Tonaufzeichnungen) können z. B. durch Einblendungen oder eine Ansage getätigt werden.

Bzgl. der Rollenverteilung hat der System-Anbieter die Einrichtung verschiedener Nutzergruppen zu ermöglichen. Zu diesen Nutzergruppen können – mit abnehmenden Zugriffsmöglichkeiten – gehören:

- Administrierende (in der Regel Lehr- oder Verwaltungspersonal der Schule, der Schulbehörde oder des Bundeslandes): Sie haben größtmögliche Zugriffsmöglichkeiten auf die Funktionen des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme. Sie verfügen bspw. über folgende Berechtigungen: Festlegung des Zeitpunktes, des Zeitrahmens und des Teilnehmerkreises der Kommunikation, Möglichkeit der Aufzeichnung der Kommunikation, Verbot der Übermittlung bestimmter den Unterricht störender Inhalte und anderer Inhalte, die im schulischen Umfeld nicht angemessen sind, Zuweisung von untergeordneten Rollen.
- Moderierende: Sie haben Zugriffsmöglichkeit auf die Funktionen des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme. Zu ihnen gehören insbesondere: Festlegung des Zeitpunktes, des Zeitrahmens und des Teilnehmerkreises der Kommunikation sowie die Zuweisung von Präsentationsrollen, Teilnehmerrollen oder Gastrollen.
- Präsentierende: Sie haben Zugriffsmöglichkeit auf die Funktionen des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme. Sie haben die Möglichkeit, Inhalte für alle Teilnehmenden zu teilen und bereitzustellen und im Rahmen von Video- und Tonkonferenzen Wortmeldungen zu steuern.
- Teilnehmende: Sie haben die Möglichkeit zur Teilnahme unter einem vorher im Rahmen eines Nutzungsprofils zugeordneten Namen. Daneben können sie die Kommunikationskanäle des Systems jedoch nur eingeschränkt zur Übermittlung von Inhalten nutzen. Ihnen steht keine Präsentationsfunktion zu.

- Gäste: Sie haben ohne Profilerstellung die Möglichkeit der Teilnehmenden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679
- DSK, Orientierungshilfe Videokonferenzsysteme
- DSK, Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
- DSK, Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- DIN SPEC 27008:2024-02 Tabelle 1, insbesondere Nr. 5.9 ff.

Nr. 16 – Identitätsmanagement (IDM)

Kriterium

1) Der System-Anbieter eines IDM stellt, wenn das IDM personenbezogene Daten an ein angebundenes schulisches Informationssystem weiterleitet bzw. ein angebundenes schulisches Informationssystem personenbezogene Daten aus dem IDM abruft, eine technische Möglichkeit bereit, die weiterzuleitenden bzw. abzurufenden personenbezogenen Daten für jedes angebundene schulische Informationssystem und für jede Rolle[61] (Lehrkraft, Schülerin und Schüler etc.) individuell freizugeben. Der System-Anbieter des IDM darf nur Daten zur Weiterleitung bzw. zum Abruf freigeben, soweit die Weiterleitung bzw. der Abruf zwischen dem Anbieter des angebundenen schulischen Informationssystems und dem System-Kunden des angebundenen schulischen Informationssystems vertraglich vereinbart wurde. Der System-Anbieter des IDM muss dies prüfen.

2) Soweit dies nach dem Stand der Technik möglich ist, hat ein IDM, das ein Single Sign-on bereitstellt, auch ein Single Log-out bereitzustellen. Die Abmeldung am IDM hat dann zur automatisierten Abmeldung an allen angebundenen Systemen zu führen.

Erläuterung

Aufgrund der Vielzahl schulischer Informationssysteme in Kombination mit der regelmäßig großen Zahl an Schülerinnen und Schülern sehen einige Bundesländer die verpflichtende Nutzung eines IDM vor. Dies beinhaltet die zielgerichtete, sichere Verwaltung und Pflege digitaler Identitäten (Sammlung personenbezogener Attribute, die eine Person im Umfeld digitaler schulischer Informationssysteme kennzeichnet) sowie die konsistente, verlässliche, ständig verfügbare und aktuelle Bereitstellung personenbezogener Daten für Schuldienste und ermöglicht die automatisierte Verwaltung der System-Nutzer, Kennungen (Authentifizierung) und benutzerbezogener Berechtigungen (Rechtvergabe).

Mittels eines IDM sollen sich Schülerinnen und Schüler, Lehrkräfte und weitere schulische Mitarbeitende authentifizieren können. Zudem kann die Rechtevergabe erleichtert über ein IDM erfolgen. Darüber hinaus können der Zweckbindungs- und Datenminimierungsgrundsatz umgesetzt werden, wenn sich die Nutzer mit ihrer digitalen ID in jedem schulischen Informationssystem, das die jeweilige Schule nutzt, authentifizieren können, ohne sich jeweils separat anmelden zu müssen.

In einigen wenigen Bundesländern erfasst der schul- und datenschutzrechtliche Regelungsbereich die Organisation von IDM. Teilweise wird nur die Möglichkeit geschaffen, ein solches zu nutzen, während in anderen Fällen die Implementierung eines IDM verpflichtend bei der Einführung von schulischen Informationssystemen vorgesehen wird, wenn diese zur Erfüllung des Erziehungs- und Bildungsauftrags erforderlich sind. In beiden Fällen sollten schulische Informationssysteme kompatibel und interoperabel mit diesen IDM bzw. deren Schnittstellen sein.

Ist die Nutzung eines IDM vorgeschrieben, schließt dies nicht aus, dass System-Anbieter anderer schulischer Informationssysteme über den Vermittlungsdienst VIDIS[62] an das IDM angebunden

[61] Wird kein Rollenkonzept für die Zugriffssteuerung verwendet, sollten vergleichbare TOM zur Rechtevergabe und zur Regelung der Datenverarbeitung angewendet werden.
[62] https://www.vidis.schule/.

werden. System-Anbieter können sich an den Vermittlungsdienst VIDIS anbinden, an den wiederum die IDM der Länder angebunden sind. VIDIS erhält dann die Daten aus dem IDM des Landes und übermittelt diese weiter an die angebundenen Systemanbieter.

Der System-Anbieter des IDM trifft keine Vorabentscheidung über die Nutzung von angebundenen Systemen durch die Schulen (System-Kunden) und System-Nutzer. Jede Schule muss individuell über jedes angebundene Angebot entscheiden können. Dabei muss es möglich sein, die Nutzung für bestimmte Personengruppen der Schule freizugeben oder einzuschränken. Es muss mindestens eine Einschränkung auf einzelne Personen und Rollen möglich sein. Bzgl. des Rollenkonzepts wird auf Nr. 3.5 verwiesen.

Die Datenweiterleitung durch das IDM an die angebundenen Dienste muss vertraglich zwischen dem System-Anbieter des IDM und dem System-Kunden (Schule) geregelt sein, s. insoweit Nr. 1.3. Wenn das IDM in ein Schulportal oder eine Lernplattform integriert ist, müssen die Verarbeitungstätigkeiten technisch und organisatorisch getrennt werden, s. Nr. 3.12.

Landesgesetzliche Regelungen

In den folgenden landesgesetzlichen Regelungen lassen sich spezifische Vorgaben bezüglich eines IDM finden:

- Berlin: § 64c SchulG und § 25 SchulDatenV Berlin enthalten Vorgaben für Fachverfahren zum Identitätsmanagement, das von der Schulaufsichtsbehörde betrieben wird.
- Mecklenburg-Vorpommern: § 5a Abs. 2-6 SchulDSV M-V.
- Saarland: § 11 SchulwDSV SL (Zentrale Identitätsverwaltung durch die Schulen, die Schulträger und die Schulaufsichtsbehörde).

Umsetzungshinweis

Einige Landesgesetze schreiben vor, welche personenbezogenen Daten im Rahmen des IDM verarbeitet werden dürfen. Dazu kann auch die Orientierungshilfe der DSK zu Online-Lernplattformen im Schulunterricht herangezogen werden, die sowohl die erforderlichen Daten zur Erfüllung des Bildungs- und Erziehungsauftrags als auch optionale Daten festhält. Der System-Anbieter sollte daher Vorkehrungen treffen, bspw. TOM vornehmen, die sicherstellen, dass keine personenbezogenen Daten über die in den Landesgesetzen aufgezählten hinaus verarbeitet werden. Den Grundsätzen der Zweckbindung und Datenminimierung folgend sollte außerdem keine doppelte Datenhaltung durch den System-Anbieter eines IDM vorgenommen werden. Wird eine bestimmte Form der Authentisierung oder Authentifizierung gefordert, bspw. eine Multi-Faktor-Authentisierung, sollte der System-Anbieter dafür sorgen, dass dies möglich ist.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 6 ff.

Nr. 17 – Digitale Klassenbücher

Kriterium

1) Der System-Anbieter von digitalen Klassenbüchern stellt durch TOM sicher, dass
    a. der System-Kunde ein Berechtigungskonzept (Rechte- und Rollenkonzept) einrichten kann, das es dem System-Kunden erlaubt, Zugriffsberechtigungen für verschiedene Nutzergruppen (z. B. Lehrkräfte und sonstiges schulisches Personal, Erziehungsberechtigte) festzulegen. Der System-Kunde muss insbesondere einstellen können, dass die digitalen Klassenbücher nur den die jeweiligen Klassen oder Lerngruppen unterrichtenden Lehrkräften zugänglich sind;
    b. der System-Kunde die Möglichkeit hat, eine Zwei-Faktor-Authentisierung zu nutzen;
    c. der System-Kunde festlegen kann, ob die verarbeiteten Daten auf lokalen Endgeräten gespeichert werden (z. B. durch Speicher- oder Exportfunktion).

2) Der System-Anbieter von digitalen Klassenbüchern stellt durch TOM sicher, dass der System-Kunde festlegen kann, welche personenbezogenen Daten – insbesondere über Schülerinnen und Schüler – verarbeitet werden können. Dabei ist auch sicherzustellen, dass Eingabefelder, die nach dem jeweiligen Landesschulrecht nicht zulässige Dateneingaben ermöglichen, durch den System-Kunden deaktivierbar sind.

Erläuterung

Das Kriterium enthält Vorgaben zur Nutzung digitaler Klassenbücher, die anstelle von Klassenbüchern in Papierform geführt werden (vgl. insbesondere § 13 Abs. 1 SchulDSVO SH).

Gesetzliche Regelungen zu digitalen Klassenbüchern finden sich nicht in allen Landesschulgesetzen. Ausführlich geregelt sind digitale Klassenbücher in Schleswig-Holstein (§ 13 SchulDSVO SH). Für Hessen finden sich z. B. Vorgaben in §§ 83, 83a SchulG-HE iVm. § 11 Abs. 1 SchDSV-HE, für Sachsen in der Ziffer II. 3. VwV Schulformulare. Die Regelungen unterscheiden sich teilweise, insbesondere auch bzgl. der Daten, die in digitalen Klassenbüchern verarbeitet werden dürfen. Dementsprechend haben die System-Anbieter sicherzustellen, dass der System-Kunde festlegen kann, welche personenbezogenen Daten verarbeitet werden können und dass nicht benötigte Eingabefelder deaktivierbar sind.

Umsetzungshinweis

Das Berechtigungskonzept (bzw. Rechte- und Rollenkonzept) sollte sich jedenfalls mit den folgenden Aspekten auseinandersetzen:

- Wem welche Rollen zugeteilt werden, z. B. für Schulleitung, Klassenlehrerin bzw. -lehrer, Administratorin bzw. Administrator, Eltern, Schülerin bzw. Schüler, Austauschschülerin bzw. -schüler, Praktikantin bzw. Praktikant.
- Wer auf welche personenbezogene Daten lesend oder schreibend zugreifen darf.
- Wer Auswertungen (z. B. bzgl. der Notenverteilung) durchführen darf und ob diese Auswertungen anonym oder personenbezogen erfolgen dürfen.

Bzgl. des Ortes, an dem die in das digitale Klassenbuch eingegebenen Daten gespeichert werden, verlangen die Länder teilweise, dass die Daten nicht lokal auf dem Gerät gespeichert werden dürfen (s. § 13 Abs. 2 Nr. 4 SchulDSVO SH). Es sollte daher z. B. die Möglichkeit bestehen, dass die Daten – je nach Wunsch des System-Kunden – auf dem Schulserver oder anderen Speichermedien gespeichert werden können.

Generell sollte das digitale Klassenbuch individuelle Einstellungsmöglichkeiten bzgl. der zu speichernden Daten und der Authentisierung (v.a. die Möglichkeit einer Zwei-Faktor-Authentisierung) aufweisen, damit die System-Kunden um den unterschiedlichen Landesvorgaben Rechnung tragen können.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Bildungsserver Rheinland-Pfalz, Digitales Klassenbuch und andere schulische Softwareprodukte, https://bildung.rlp.de/schulemedienrecht/themen/unterrichtsorganisation-und-klassenverwaltung/digitales-klassenbuch-und-andere-schulische-softwareprodukte (Stand: Februar 2026).
- HBDI, Verzeichnis von Verarbeitungstätigkeiten, hier: digitales Klassenbuch: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2024-02/verfahrensverzeichnis_klassenbuch_digital_v1.0.pdf (Stand: Februar 2026).
- Kultusministerium Baden-Württemberg, Datenschutzrechtliche Hinweise zur Nutzung eines elektronischen Tage- oder Klassenbuchs (ETB): https://bb.schulamt-bw.de/site/pbs-bw-rebrush2024/get/documents_E20250160/KULTUS.Dachmandant/KULTUS/Schulaemter/schulamt-boeblingen/1%20%C3%9Cber%20uns/Personalrat/dl_%C3%B6pr_etb/2023-07-29%20Datenschutzrechtliche%20Hinweise%20elektronisches%20Tagebuch%20Klassenbuch_07_23.pdf (Stand: Februar 2026).
- LfD Niedersachsen, Hinweise zur Einführung eines elektronischen Klassenbuchs des: https://www.lfd.niedersachsen.de/download/115587/Hinweise_zur_Einfuehrung_eines_elektronischen_Klassenbuchs_Stand_03.09.2018_.pdf (Stand: Februar 2026).

Landesgesetzliche Regelungen

- Hessen: §§ 83, 83a SchulG-HE iVm. § 11 Abs. 1 SchDSV-HE.
- Sachsen: Ziffer II. 3. VwV Schulformulare Sachsen.
- Schleswig-Holstein: § 13 SchulDSVO SH.

Nr. 18 – Automatisierte Entscheidungsfindung und Künstliche Intelligenz in schulischen Informationssystemen
(insbesondere Art. 22 DS-GVO)

Kriterium

1) Der System-Anbieter verarbeitet personenbezogene Daten von Schülerinnen und Schülern, Lehrkräften, sonstigem Personal und Erziehungsberechtigten nicht als Trainings-, Validierungs- und Testdaten für KI-Systeme.

2) Kann das schulische Informationssystem Entscheidungen über System-Nutzer treffen, die Auswirkungen auf deren schulischen Werdegang haben können (z. B. Schulnoten), stellt der System-Anbieter sicher, dass die Entscheidung durch einen Menschen überprüft und abgeändert werden kann. Es muss nachvollziehbar sein, wie das System die Entscheidung getroffen hat.

3) Handelt es sich bei dem schulischen Informationssystem um ein Hochrisiko-KI-System, unterstützt der System-Anbieter den System-Kunden bei der Verwendung der Informationen gemäß Art. 13 KI-VO im Rahmen der vom System-Kunden durchzuführenden Datenschutz-Folgenabschätzung.

Erläuterung

Der Einsatz Künstlicher Intelligenz und algorithmenbasierter Entscheidungssysteme geht häufig mit einer umfangreichen Verarbeitung personenbezogener Daten einher. Aufgrund der potenziell hohen Aussagekraft der Datenverarbeitung besteht ein hohes Risiko für die Rechte und Freiheiten der Schülerinnen und Schüler. Dies ist z. B. der Fall, wenn Künstliche Intelligenz für Learning Analytics eingesetzt wird.

Künstliche Intelligenz wird von der technikneutralen DS-GVO nicht gesondert geregelt. Es gelten die allgemeinen Regelungen der DS-GVO.

Im Zusammenhang mit Künstlicher Intelligenz und algorithmenbasierten Entscheidungssystemen kommt Art. 22 DS-GVO eine hohe Bedeutung zu. Nach Art. 22 Abs. 1 und 2 DS-GVO bedarf eine Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht, einer Rechtsgrundlage, wenn von ihr eine rechtliche Wirkung ausgeht oder sie die betroffenen Personen in ähnlicher Weise erheblich beeinträchtigt. Eine solche Wirkung bzw. Beeinträchtigung ist bei Auswirkungen auf den schulischen Werdegang zu bejahen. Dies betrifft u.a. Verhaltens- und Leistungskontrollen (z. B. bei Benotungen oder anderen Formen der Beurteilung) sowie Entscheidungen über den schulischen Werdegang. Hierfür sind (derzeit) keine Rechtsgrundlagen ersichtlich. Weder ist der Einsatz für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich (Art. 22 Abs. 2 lit. a DS-GVO) noch besteht eine explizite gesetzliche Grundlage (lit. b). Auch eine Einwilligung ist im schulischen Kontext (Vormittagsmarkt) mangels Freiwilligkeit nicht möglich (lit. c). Jedenfalls aber haben schulische Informationssystem eine menschliche Intervention zu ermöglichen (vgl. Art. 22 Abs. 3 DS-GVO: „Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört").

Beim Einsatz schulischer Informationssysteme verarbeitete personenbezogene Daten von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten dürfen nicht als Trainings-, Validierungs- und Testdaten für KI-Systeme verwendet werden, da hierfür (derzeit) keine Rechtsgrundlage besteht. Insbesondere kommt eine Einwilligung aufgrund des besonderen Gewaltverhältnisses im schulischen Kontext (Vormittagsmarkt) nicht in Betracht. Nicht ausgeschlossen wird hierdurch die Verwendung von nicht-personenbezogenen Daten als Trainings-, Validierungs- und Testdaten; dies betrifft insbesondere anonymisierte Daten (s. EG 26 Satz 5 und 6 DS-GVO).

Gemäß Art. 26 Abs. 9 KI-VO verwendet der Betreiber eines Hochrisiko-KI-Systems die gemäß Art. 13 KI-VO bereitgestellten Informationen, um seiner Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO nachzukommen. Betreiber i.d.S. ist gemäß Art. 3 Nr. 4 KI-VO eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet. Stellt der System-Anbieter dem System-Kunden, also der Schule, ein schulisches Informationssystem zur Verfügung, bei dem es sich um ein Hochrisiko-KI-System i.S.v. Art. 3 Nr. 1 i.V.m. Art. 6 KI-VO handelt (insbesondere Art. 6 Abs. 2 i.V.m. Anhang III Nr. 3 KI-VO), ist davon auszugehen, dass die Schule (zumindest auch) Betreiberin des KI-Systems ist, wenn sie dieses im Rahmen ihrer Aufgabenwahrnehmung (v.a. Bildung und Erziehung, Verwaltung etc.) eigenverantwortlich nutzt (und dabei insbesondere über die Ein- und Ausgaben des KI-Systems entscheidet).

Die Pflicht zur Durchführung der Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO betrifft in der hier relevanten Konstellation den System-Kunden (also die Schule) als datenschutzrechtlich Verantwortlichen. Der System-Kunde hat daher die Informationen nach Art. 13 KI-VO bei der Datenschutz-Folgenabschätzung zu verwenden. Der System-Anbieter unterstützt (vgl. auch Nr. 10) den System-Kunden nach Kräften bei Verwendung der Informationen nach Art. 13 KI-VO.

Werden im Rahmen des Einsatzes von KI-Systemen personenbezogene Daten an Drittländer oder internationale Organisationen übermittelt, gelten die Vorgaben in Nr. 14.

Landesgesetzliche Regelungen

- Saarland: § 6 SchulwDSG SL (Verarbeitung mit Profilingmöglichkeit)

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe Künstliche Intelligenz und Datenschutz
- BayLDA, KI & Datenschutz
- LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz
- HmbBfDI, Checkliste zum Einsatz LLM-basierter Chatbots
- CNIL, AI system development: CNIL's recommendations to comply with the GDPR
- CNIL, AI how-to sheets

Kapitel VI: Werbe- und Cookieverbot

Nr. 19 – Werbe- und Cookieverbot

(Art. 25 Abs. 2, Art. 5 Abs. 1 lit. b DS-GVO sowie Art. 95 DS-GVO)

Kriterium

1) Der System-Anbieter verarbeitet personenbezogene Daten nicht zu Zwecken der Werbung oder zu anderen kommerziellen Zwecken. Eine Verarbeitung zur Verbesserung des konkret eingesetzten schulischen Informationssystems wird hiervon nicht erfasst.

2) Die Speicherung von Informationen auf Endgeräten der System-Nutzer oder der Zugriff auf Informationen, die bereits auf den Endgeräten gespeichert sind, ist nur zulässig, wenn die Speicherung oder der Zugriff unbedingt erforderlich ist, um das schulische Informationssystem zur Verfügung stellen zu können. Der System-Anbieter stellt durch TOM sicher, dass eine Speicherung nicht erforderlicher Informationen auf dem Endgerät des System-Nutzers unterbleibt.

Erläuterung

Kinder genießen bei der Verarbeitung ihrer personenbezogenen Daten im Rahmen der DS-GVO besonderen Schutz, wie insbesondere EG 38 DS-GVO hervorhebt. Dieser besondere Schutz verbietet

grundsätzlich die Verwendung personenbezogener Daten von Kindern zu Werbezwecken oder anderen kommerziellen Zwecken. Daher muss der System-Anbieter sicherstellen, dass das schulische Informationssystem so ausgestaltet ist, dass personenbezogene Daten nicht zu Zwecken der Werbung (d.h. Äußerungen, die auf die Förderung des Absatzes von Waren oder Dienstleistungen einer wirtschaftlich tätigen Person gerichtet sind[63]) oder zu anderen kommerziellen Zwecken (z. B. Verkauf der Daten an Adresshändler) verarbeitet werden. Dieses Werbeverbot soll dazu beitragen, die Nutzung von schulischen Informationssystemen im Rahmen des schulischen Lehr- und Lernbetriebes werbefrei zu halten.

Keine unzulässigen kommerziellen Zwecke i.S. dieses Kriteriums sind die Zwecke, die im direkten Zusammenhang mit der Erbringung der vertraglich festgelegten Leistung des System-Anbieters stehen. Eine Verwendung der Daten zur Verbesserung des konkret eingesetzten schulischen Informationssystems soll durch das Kriterium nicht unterbunden werden.

Die Speicherung von Cookies (und vergleichbaren Informationen) in den Endeinrichtungen (z. B. Smartphones, Laptops, PCs, s. § 2 Abs. 2 Nr. 6 TDDDG; im Kriterium als Endgeräte bezeichnet) der Endnutzer (d.h. Schülerinnen und Schüler etc.) ist nach § 25 TDDDG (i.V.m. Art. 5 Abs. 3 RL 2002/58/EG[64]) zulässig, wenn die Endnutzer eingewilligt haben (§ 25 Abs. 1 TDDDG) oder wenn sie unbedingt erforderlich ist, damit der System-Anbieter einen ausdrücklich gewünschten Dienst zur Verfügung stellen kann (§ 25 Abs. 2 Nr. 2 TDDDG).[65] Im schulischen Kontext ist eine freiwillige Einwilligung regelmäßig nicht anzunehmen (s. die Erläuterungen zu Nr. 5.2). Daher dürfen nur unbedingt erforderliche Cookies gesetzt werden.

Landesgesetzliche Regelungen

Aus den Landesschul- und Landesdatenschutzgesetzen ergibt sich im Wesentlichen, dass Schulen personenbezogene Daten in bestimmten Situationen zur Erfüllung ihres Erziehungs- und Bildungsauftrags und für schulorganisatorische Maßnahmen verarbeiten dürfen (s. hierzu insbesondere Nr. 5.2), nicht aber für kommerzielle Zwecke.

Umsetzungshinweis

Der System-Anbieter hat durch TOM zu gewährleisten, dass die personenbezogenen Daten im Rahmen der Nutzung eines schulischen Informationssystems nicht zu Zwecken der Werbung oder zu anderen kommerziellen Zwecken verarbeitet werden. Dies sollte i.S.v. Art. 25 Abs. 2 DS-GVO (s. Nr. 20) bereits vor der Nutzung des Systems voreingestellt sein.

Für den Fall der Verarbeitung personenbezogener Daten zur Verbesserung des schulischen Informationssystems sollte der System-Anbieter i.S.v. Art. 5 Abs. 1 lit. c DS-GVO auf gängige Methoden zur Datenminimierung zurückgreifen, insbesondere auf die Maßnahmen der Pseudonymisierung oder Anonymisierung sowie die Möglichkeit, personenbezogene Daten nur aggregiert zu verarbeiten.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)

[63] S. z. B. Art. 2 lit. a Richtlinie 2006/114/EG.
[64] S. hierzu bzgl. des Zertifizierungsmaßstabes das Begleitdokument Zertifizierungsgegenstand
[65] S. zudem § 25 Abs. 2 Nr. 1 TDDDG zur Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz.

Kapitel VII: Anforderungen an die Systemgestaltung

Nr. 20 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 20.1 – Datenschutz durch Systemgestaltung
(Art. 25 Abs. 1 DS-GVO i.V.m. Art. 5 Abs. 1 DS-GVO)

Kriterium

1) Der System-Anbieter führt eine Risikoanalyse auf Grundlage des Risikobewertungskonzepts oder eines anderen Verfahrens zur Risikobewertung für alle Verarbeitungsvorgänge des schulischen Informationssystems durch und muss dabei auf die besonderen schulischen Gegebenheiten Rücksicht nehmen. Die Risikoanalyse umfasst die Ermittlung der Wahrscheinlichkeit sowie die potenziellen Auswirkungen der identifizierten Risiken auf die Rechte und Freiheit der betroffenen Personen.

2) Unter Berücksichtigung der ermittelten Risiken verfügt der System-Anbieter zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung über TOM zur praktikablen, zielführenden und wirksamen Umsetzung der Grundsätze des Art. 5 DS-GVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht), um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen – auch in den verlängerten Leistungsketten durch etwaige Auftragsverhältnisse – zu schützen.

3) Bei der Implementierung der TOM berücksichtigt der System-Anbieter insbesondere den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen.

4) Der System-Anbieter muss nachweisen können, dass die implementierten TOM zu einer wirksamen Umsetzung der Grundsätze des Art. 5 DS-GVO führen.

Erläuterung

Der System-Kunde muss als Verantwortlicher die Gestaltungspflicht aus Art. 25 Abs. 1 DS-GVO erfüllen. Er darf gemäß Art. 28 Abs. 1 DS-GVO nur System-Anbieter als Auftragsverarbeiter auswählen, die die Erfüllung dieser Pflicht ermöglichen und nachweisen. Technik und Organisation des schulischen Informationssystems sind daher so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DS-GVO bestmöglich und nachweislich unterstützen.

Der EDSA betont die Bedeutung einer wirksamen Umsetzung der Datenschutzgrundsätze durch den Verantwortlichen. Er äußert sich in den Leitlinien 4/2019 wie folgt:

„Wirksamkeit ist der Kern des Konzepts des Datenschutzes durch Technikgestaltung. Die Anforderung zur wirksamen Umsetzung der Grundsätze bedeutet, dass die Verantwortlichen die für den Schutz dieser Grundsätze erforderlichen Maßnahmen und Garantien umsetzen müssen, um die Rechte der betroffenen Personen zu gewährleisten. Jede umgesetzte Maßnahme sollte zu den beabsichtigten Ergebnissen für die vom Verantwortlichen vorgesehene Verarbeitung führen. Aus dieser Feststellung ergeben sich zwei Konsequenzen.

Zum einen, dass Artikel 25 [DS-GVO] nicht die Umsetzung bestimmter technischer und organisatorischer Maßnahmen vorsieht, sondern dass die gewählten Maßnahmen und Garantien speziell für die Umsetzung der Datenschutzgrundsätze bei der betreffenden konkreten Verarbeitung angelegt sein sollten. Dabei sollte bei den Maßnahmen und Garantien die Wirksamkeit im Vordergrund stehen, und der Verantwortliche sollte weitere Maßnahmen umsetzen können, um einer etwaigen Risikoerhöhung Rechnung tragen zu können. Die Wirksamkeit von Maßnahmen hängt daher von den Rahmenbedingungen der betreffenden Verarbeitung und von einer Prüfung bestimmter Aspekte ab, die bei der Festlegung der Mittel für die Verarbeitung zu berücksichtigen sind. […]

Zum anderen sollten die Verantwortlichen nachweisen können, dass die Grundsätze gewahrt wurden.

Die umgesetzten Maßnahmen und Garantien sollten die gewünschte Wirkung in Bezug auf den Datenschutz erzielen; und der Verantwortliche sollte über eine Dokumentation der umgesetzten technischen und organisatorischen Maßnahmen verfügen. Hierfür kann der Verantwortliche geeignete zentrale Leistungsindikatoren zum Nachweis der Wirksamkeit festlegen. Ein zentraler Leistungsindikator ist ein vom Verantwortlichen gewählter messbarer Wert, der Auskunft über die Wirksamkeit des Verantwortlichen bei der Erreichung seiner Datenschutzziele gibt. Die zentralen Leistungsindikatoren können quantitativ sein, wie z. B. der Prozentsatz von falsch-positiven oder falsch-negativen Ergebnissen, die Reduzierung von Beschwerden, die Verkürzung der Zeit für Antworten an betroffene Personen, die ihre Rechte wahrnehmen, oder qualitativ, wie z. B. Bewertungen der Leistung, die Verwendung von Bewertungsskalen oder Beurteilungen durch Sachverständige. Als Alternative zu den zentralen Leistungsindikatoren können die Verantwortlichen unter Umständen den Nachweis der wirksamen Umsetzung der Grundsätze dadurch erbringen, dass sie Sinn und Zweck ihrer Prüfung der Wirksamkeit der gewählten Maßnahmen und Garantien erläutern."[66]

Die wirksame Umsetzung der Grundsätze ist mit jeweils geeigneten Methoden nachzuweisen. So ist eine wirksame Umsetzung des Vertraulichkeitsprinzips (Art. 5 Abs. 1 lit. f DS-GVO) durch kryptographische Verfahren mit entsprechenden mathematischen Verfahren nachzuweisen. Gleiches gilt für die wirksame Umsetzung der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) durch technische Anonymisierungsverfahren (etwa k-Anonymität oder Differential Privacy). Die Umsetzung von Transparenz- und/oder Interventionsmöglichkeiten betroffener Personen (Art. 5 Abs. 1 lit. a i.V.m. den Betroffenenrechten gemäß Art. 12 ff. DS-GVO), deren Wirksamkeit von ihrer Bedienbarkeit („Usability") durch Laien abhängt, kann über empirische Konzepte und Methoden aus der User Experience- bzw. Mensch-Maschine-Interaktionsforschung, Psychologie und/oder Verhaltensökonomik nachgewiesen werden. Wird der Nachweis von Dritten übernommen, ist darzulegen, wieso und inwiefern der Nachweis für das vorliegende, zu zertifizierende Verfahren übernommen werden kann und deshalb kein eigener Nachweis durchgeführt werden muss.

Wie vom EDSA ausgeführt (s.o.), schließt der Nachweis der Wirksamkeit sowohl qualitative als auch quantitative Methoden ein. Die Wahl der jeweiligen Methode hängt dabei von der Fragestellung ab. Geht es primär darum, explorativ herauszufinden, welche Erwartungen die Betroffenen an den Schutz vor den Risiken der Datenverarbeitung haben, bieten sich zunächst qualitative Methoden wie etwa Interviews und Workshops mit Betroffenen an, die die entsprechenden Wieso-, Weshalb-, Warum-Fragen erlauben. Anhand dieser Erkenntnisse lassen sich dann entsprechende Prototypen für Schutzmaßnahmen entwickeln (z. B. visuelle Mockups oder Clickdummies), die wiederum qualitativ auf ihre Wirksamkeit getestet werden können. Stellen sich in diesem Prozess hinreichend begründete Hypothesen für eine oder mehrere mögliche ausreichend wirksame Schutzmaßnahmen heraus, können diese schließlich im Rahmen quantitativer Tests mit Blick auf ihre Repräsentativität verifiziert bzw. falsifiziert werden. Hierfür kommen sogenannte A/B-Tests in Betracht, in deren Rahmen verschiedene Varianten einer Schutzmaßnahme in Bezug auf ihre Wirksamkeit verglichen werden können. Die so festgestellte wirksamste Schutzmaßnahme stellt dann den jeweils geltenden Stand der Technik dar.

Liegt allgemein noch kein Nachweis vor, muss der System-Anbieter diesen selbst liefern. Der Umfang des Nachweises richtet sich nach dem Ausmaß der festgestellten Risiken sowie den Kosten. Je umfassender die Risiken für die betroffenen Personen sind, desto mehr Mühe muss der System-Anbieter auf den Nachweis verwenden, dass seine Schutzmaßnahmen wirksam sind. Dem darf er andererseits die Kosten gegenüberstellen, was bei unverhältnismäßig hohen Kosten zu einer Entlastung der Nachweispflicht führen kann.

Bei der Umsetzung der TOM berücksichtigt der System-Anbieter gemäß Art. 25 Abs. 1 DS-GVO insbesondere den Stand der Technik und die Implementierungskosten.

Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen. Soweit es in Bezug auf die festgestellten

[66] EDSA, Leitlinien 4/2019, S. 6.

Risiken und die zu ihrer wirksamen Kontrolle der jeweils technisch-organisatorisch umzusetzenden Norm noch keinen Stand der Technik gibt, kann auf die anerkannten Regeln der Praxis zurückgegriffen werden.

Bei der Bestimmung der TOM ist zu berücksichtigen, dass die Implementierungskosten nicht als Grund dafür herangezogen werden dürfen, Datenschutz durch Technikgestaltung gar nicht umzusetzen.

Umsetzungshinweis

Zur Erfüllung der Anforderungen von Art. 25 Abs. 1 DS-GVO ist es unabdingbar, diese bereits bei der Modellierung der schulischen Informationssysteme und Verarbeitungsvorgänge auf allen Ebenen zu berücksichtigen. Dabei ist die Risikoanalyse (s. Begleitdokument) Voraussetzung, um anschließend risikoangemessene TOM festzulegen. Diese Risikoanalyse sollte bisher ergriffene TOM berücksichtigen.

Für den Nachweis der Wirksamkeit der jeweiligen TOM kann auf empirische Methoden zurückgegriffen werden (siehe hierzu bereits zuvor bei der Erläuterung). In der aktuellen Praxis liegt ein Fokus häufig auf technischen Schutzmaßnahmen wie z. B. der Anonymisierung der Daten. Hierbei darf nicht übersehen werden, dass diese häufig die pädagogische Arbeit der Lehrkräfte erschweren oder sogar vereiteln können. Der Fokus sollte daher verstärkt auch organisatorische Schutzmaßnahmen in Betracht ziehen, z. B. leicht verständliche Handlungsempfehlungen an die Lehrkräfte und/oder nutzerfreundlichere Ausgestaltungen der Systeme, die den datenschutzkonformen Gebrauch in der Praxis sicherstellen (einschließlich entsprechender Gebrauchsanleitungen).

Der Grundsatz der datenschutzfördernden Systemgestaltung verlangt eine Beachtung operativer Datenschutzanforderungen bereits während der Planungsphase, damit nicht-datenschutzkonforme Funktionen gar nicht erst implementiert und nachträglich abgestellt werden müssen. Nach dem SDM können zur datenschutzgerechten Gestaltung der Verarbeitungsvorgänge die Gewährleistungsziele des SDM (C1.1 bis C1.7) als Design-Prinzipien oder -Strategien interpretiert werden. Es sind ausgereifte Changemanagement-Prozesse erforderlich, um auf Änderungen der rechtlichen Rahmenbedingungen reagieren und um neue, datenschutzfreundliche Techniken in vorhandene Verarbeitungssystemen einsetzen zu können. Hierzu zählen bspw. Privacy Enhancing Technologies (PETs), die in schulischen Informationssystemen zum Einsatz kommen können.

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Sie reichen von der Implementierung eines datensparsamen Logins für den Zugang zum schulischen Informationssystem, über Rollen- und Berechtigungskonzepte für die Nutzung und Administration des Systems (s. Nr. 3.5 zur Zugriffskontrolle) bis hin zu Löschkonzepten für die Löschung der Daten (s. Nr. 7.5 zur Löschung und Nr. 1.9 sowie Nr. 12 zur Rückgabe und Löschung von Datenträgern). Dazu sollte der System-Anbieter die Orientierungshilfe der DSK zu Online-Lernplattformen im Schulunterricht[67] berücksichtigen. Diese macht Vorgaben für Schulen, aber auch explizit für System-Anbieter, damit diese ihre schulischen Informationssysteme so gestalten und anpassen können, damit diese datenschutzkonform in den Schulen zum Einsatz kommen können.

Zu den weiteren Maßnahmen, die System-Anbieter ergreifen sollten, gehören Maßnahmen zur Datenminimierung, wodurch nur die für die Aufgabenerfüllung erforderlichen Daten verarbeitet werden, oder auch Pseudonymisierungsvorkehrungen (s. Nr. 1.7 und Nr. 3.9 zur Pseudonymisierung).

Auch Maßnahmen, die es der betroffenen Person ermöglichen, ihre Betroffenenrechte möglichst einfach auszuüben, zählen hierzu, da sie Transparenz und Kontrollmöglichkeiten für diese erhöhen (s. Nr. 7 zur Unterstützung des System-Kunden durch den System-Anbieter bei der Erfüllung der Betroffenenrechte). Beispielhafte Maßnahmen sind die Antragstellung auf Auskunft nach Art. 15 Abs. 1 DS-GVO auf Knopfdruck innerhalb des Systems oder der Onlineabruf von Daten, die zur betroffenen Person gespeichert sind.

Der System-Anbieter sollte die Abwägungsvorgänge dokumentieren, die ihn bei der Auswahl der TOM zur Gewährleistung der Datenschutzgrundsätze geleitet haben, da er bei dieser Auswahl den Stand der Technik, die Implementierungskosten, die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Personen in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen muss.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

[67] DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 6ff.

- EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art.-29-Gruppe, WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679
- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht
- SDM, Abschnitt D1 Generische Maßnahmen
- SDM-Baustein 41 „Planen und Spezifizieren“
- SDM-Baustein 42 „Dokumentieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur
- ISO/IEC 27002:2022 Ziff. 8.25 Lebenszyklus einer sicheren Entwicklung
- ISO/IEC 27002:2022 Ziff. 8.27 Sichere Systemarchitektur und technische Grundsätze
- ISO/IEC 27701:2025 Ziff. B.2.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- ISO/IEC 27701:2025 Ziff. B.3.27 Lebenszyklus einer sicheren Entwicklung
- ISO/IEC 27701:2025 Ziff. B.3.29 Sichere Systemarchitektur und technische Grundsätze
- BSI, IT Grundschutz Kompendium, CON 2 Datenschutz

Nr. 20.2 – Datenschutz durch datenschutzfreundliche Voreinstellungen
(Art. 25 Abs. 2 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch Voreinstellungen im jeweiligen schulischen Informationssystem sicher, dass nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck im Hinblick auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung erforderlich sind. Er stellt zudem sicher, dass auch der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird, das erforderlich ist, um den Verarbeitungszweck des System-Kunden zu erfüllen. In Bezug auf Letzteres muss der System-Anbieter sicherstellen, dass Personen, die unter seiner Aufsicht handeln, nur auf einer Need-To-Know-Basis auf personenbezogene Daten zugreifen können, d.h. wenn sie diese kennen müssen.

2) Der System-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Erläuterung

Der Verantwortliche hat gemäß Art. 25 Abs. 2 DS-GVO geeignete TOM zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Er darf nur Anbieter schulischer Informationssysteme auswählen, die die Erfüllung dieser Pflicht ermöglichen. Die Voreinstellungen des schulischen Informationssystems sind daher so zu wählen, dass sie Art. 25 Abs. 2 DS-GVO genügen.

Umsetzungshinweis

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Der System-Anbieter hat durch Voreinstellungen sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, die für den jeweilig bestimmten Verarbeitungszweck erforderlich sind. Hierzu sollte nicht nur die Menge der verarbeiteten Daten minimiert werden, sondern auch der Umfang ihrer Verarbeitung,

ihre Speicherfrist und ihre Zugänglichkeit. Muss bspw. die Nutzung des schulischen Informationssystems protokolliert werden, um Missbrauch aufzudecken oder die Datensicherheit sicherzustellen, so sollte die Voreinstellung derart gewählt werden, dass die Daten anonymisiert erhoben und verarbeitet werden.

Videokonferenzsysteme und andere digitale Kommunikationssysteme müssen beispielsweise so gestaltet sein, dass sie nur die Daten verarbeiten, die für die Bereitstellung des Kommunikationsdienstes zwingend erforderlich sind. Die Aufnahmegeräte sind beim Beitritt deaktiviert; siehe hierzu Nr. 15.

System-Nutzer bzw. System-Kunden können von den datenschutzfreundlichen Voreinstellungen abweichen, wenn sie z. B. umfangreichere Verarbeitungsoptionen wünschen. Hierfür ist eine gute Nutzbarkeit des schulischen Informationssystems ebenso wichtig wie eine Information des System-Kunden darüber, welche Auswirkungen Änderungen von Voreinstellungen haben können (z. B. über Pop-up-Fenster innerhalb des Dienstes). Art. 25 Abs. 2 DS-GVO verpflichtet jedoch dazu, dass die umfangreicheren Verarbeitungsoptionen nicht voreingestellt sind, sondern vom System-Kunden bei Bedarf eingeschaltet und aktiviert werden können. Soweit der System-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Anforderungen an die Voreinstellungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht
- DSK, Orientierungshilfe Videokonferenzsysteme
- SDM, Abschnitt D1 Generische Maßnahmen
- SDM-Baustein 41 „Planen und Spezifizieren“
- SDM-Baustein 42 „Dokumentieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur
- ISO/IEC 27701:2025 Ziff. B.2.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Anlagen

1. Listen nach Art. 35 Abs. 4 DS-GVO zur Datenschutz-Folgenabschätzung

Der System-Anbieter ist verpflichtet, die folgenden Angaben vor Verwendung auf Aktualität zu prüfen (Stand 01.03.2026).

- Bayern (Bayerischer LfD)
  - Öffentlicher Bereich: https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf
- Baden-Württemberg (LfDI Baden-Württemberg)
  - Nicht-öffentlicher Bereich: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf
- Berlin (Berliner DSB)
  - Öffentlicher Bereich: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2018-BlnBDI_DSFA-oeffentlich.pdf
  - Nicht-öffentlicher Bereich: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2018-BlnBDI_DSFA-nicht-oeffentlich.pdf
- Brandenburg (LDA Brandenburg)
  - Nicht-öffentlicher Bereich: https://www.lda.brandenburg.de/sixcms/media.php/9/DSFA-Liste_nicht_%C3%B6ffentlicher_Bereich.pdf
  - Öffentlicher Bereich: https://www.lda.brandenburg.de/sixcms/media.php/9/DSFA-Liste_%C3%B6ffentlicher_Bereich.pdf
- Bremen (LfDI Bremen)
  - Nicht-öffentlicher Bereich: https://www.datenschutz.bremen.de/sixcms/media.php/13/DSFA%20Muss-Liste%20LfDI%20HB.pdf
- Hamburg (HmbBfDI)
  - Öffentlicher Bereich: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/Liste_Art_35-4_DSGVO_HmbBfDI-oeffentlicher_Bereich_v2.0a.pdf
  - Nicht-öffentlicher Bereich: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/DSFA_Muss-Liste_fuer_den_nicht-oeffentlicher_Bereich_-_Stand_17.10.2018.pdf
- Hessen (Hessischer Beauftragter für Datenschutz und Informationsfreiheit)
  - Ohne Differenzierung: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/dsfa_muss_liste_dsk_de.pdf
- Mecklenburg-Vorpommern (LfDI Mecklenburg-Vorpommern)
  - Öffentlicher Bereich: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/MV-DSFA-Muss-Liste-Oeffentlicher-Bereich.pdf
  - Nicht-öffentlicher Bereich: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/ListevonVerarbeitungsvorgaengen-nachArt35Abs4DS-GVO/DE_DSFA_Muss-Liste.pdf
- Niedersachsen (LfD Niedersachsen)

- Öffentlicher Bereich: https://www.lfd.niedersachsen.de/download/134414/DSFA_Muss-Liste_fuer_den_oeffentlichen_Bereich.pdf
- Nicht-öffentlicher Bereich: https://www.lfd.niedersachsen.de/download/134415/DSFA_Muss-Liste_fuer_den_nicht-oeffentlichen_Bereich.pdf

- Nordrhein-Westfalen (LDI Nordrhein-Westfalen)
  - Öffentlicher Bereich: https://www.ldi.nrw.de/system/files/media/document/file/liste-art-35-4-nrw-oeb_v2_3.pdf
  - Nicht-öffentlicher Bereich: https://www.ldi.nrw.de/system/files/media/document/file/dsk_dsfa_muss-liste_version_1_1_deutsch_4.pdf
- Rheinland-Pfalz (LfDI Rheinland-Pfalz)
  - Öffentlicher Bereich: https://www.datenschutz.rlp.de/fileadmin/datenschutz/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_OE.pdf
  - Nicht-öffentlicher Bereich: https://www.datenschutz.rlp.de/fileadmin/datenschutz/Dokumente/Orientierungshilfen/DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- Saarland (Unabhängiges Datenschutzzentrum Saarland)
  - Ohne Differenzierung: https://www.datenschutz.saarland.de/themen/datenschutz-folgenabschaetzung
- Sachsen (SDTB Sachsen)
  - Ohne Differenzierung (unter Verweis auf DSK): https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- Sachsen-Anhalt (LfD Sachsen-Anhalt)
  - Öffentlicher Bereich: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Internationales/Datenschutz-Grundverordnung/Liste_DSFA/Art-35-Liste-oeffentlicher_Bereich.pdf
  - Nicht-öffentlicher Bereich: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Internationales/Datenschutz-Grundverordnung/Liste_DSFA/Art-35-Liste-nichtoeffentlicher_Bereich.pdf
- Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
  - Ohne Differenzierung: https://www.datenschutzzentrum.de/uploads/dsgvo/2018_10_17_DSK_DSFA-Liste-1_1.pdf
- Thüringen (TLfDI)
  - Öffentlicher und nicht-öffentlicher Bereich: https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf
- Bundesrepublik Deutschland (BfDI)
  - Öffentlicher Bereich: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf?__blob=publicationFile&v=7
- Datenschutzkonferenz (DSK)
  - DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist (für den nicht-öffentlichen Bereich), https://www.lfd.niedersachsen.de/download/134415/DSFA_Muss-Liste_fuer_den_nicht-oeffentlichen_Bereich.pdf. Die Liste der DSK wird von allen Datenschutzaufsichtsbehörden der Bundesländer verwendet

2. Aufbewahrungs- und Löschfristen der Landesgesetze in Jahren

Der System-Anbieter ist verpflichtet, die folgenden Angaben vor Verwendung auf Aktualität zu prüfen (Stand 01.03.2026).

Bundesland	Grunddaten (Schülerkarteikarten; Schülerlisten; Schülerbogen; Schülerstammblätter)	Abschluss- und Abgangszeugnisse	Prüfungsunterlagen/ Prüfungsakten	Schülerakten	Konferenzen	Notenlisten/ Zeugnisse	sonderpädagogische Gutachten/ sonderpädagogische Maßnahmen	Lern- und Förderpläne	Schulübergangsempfehlungen/ Schullaufbahnbogen	Klassenbücher/ Kurshefte
Baden-Württemberg	60	60	5	2	/**	2	2	2	2	5
Bayern	50	50	2	50	1*	1	1	1	1	1
Berlin	2/1	60	10	5	/**	5	5	2	10	10/2
Brandenburg	5	40	/**	10	/**	3	5	1	1	3
Bremen	/**	50	10	50	10/5	3	/**	3	3	3
Hamburg	20/3	55	20/3	3	/**	3	3	3	3	3
Hessen	50	50	10	50/5	30	5	/**	/**	/**	5
Mecklenburg-Vorpommern	15	45	5*	5*	5*	15	5*	5*	5*	15
Niedersachsen	50/1	50	2	1*	1*	1*	2	4	1*	1*
Nordrhein-Westfalen	20	50	10	5*	5*	10	5*	5*	5*	10
Rheinland-Pfalz	/**	/**	/**	/**	/**	/**	/**	/**	/**	/**
Saarland	50	50	5*	5*	/**	50	5*	5*	5*	5*
Sachsen	20	50	10	/**	5	20	/**	/**	/**	10
Sachsen-Anhalt	10	45	10	2*	10/5	2	2*	2*	2*	2
Schleswig-Holstein	55	40	10	2	/**	10	2	2	2	3
Thüringen	20	50	10/5/2	/**	/**	/**	/**	/**	/**	2

Bundesland	Einwilligungserklärungen (Veröffentlichung von Fotos)	Erziehungsmaßnahmen	Fehlzeiten/ Entschuldigungen/ Anwesenheits- nachweise	PbD auf privaten Endgeräten der Lehrkräfte	Akten des pädagogischen Personals	Schriftverkehr
Baden-Württemberg	5	/**	1	1	/**	/**
Bayern	1	1	1	1	/**	/**
Berlin	/**	3	2	/**	2	/**
Brandenburg	5	/**	5	5	2	/**
Bremen	/**	/**	/**	1	10/5	5
Hamburg	/**	/**	/**	/**	10/5	/**
Hessen	/**	2/1	2	/**	/**	/**
Mecklenburg-Vorpommern	5*	5*	5*	5*	5*	5*
Niedersachsen	1*	1*	1	1*	1*	1*
Nordrhein-Westfalen	5*	5*	5*	5*	5*	5*
Rheinland-Pfalz	/**	/**	/**	/**	/**	/**
Saarland	5*	5*	5*	5*	5*	5*
Sachsen	/**	/**	/**	/**	5	10
Sachsen-Anhalt	2*	2*	2*	2*	/**	/**
Schleswig-Holstein	/**	/**	/**	/**	/**	/**
Thüringen	/**	/**	/**	/**	/**	/**

Diese Liste dient dazu, einen Überblick über die Aufbewahrungs- und Löschpflichten gemäß der Landesgesetze zu geben. Die Darstellung ist teilweise vereinfacht ist und kann keinen Anspruch auf Vollständigkeit oder Aktualität stellen.

*Erfasst durch die Auffangregelung, wonach andere als die genannten Daten für eine festgelegte Anzahl von Jahren zu speichern sind

** Lösch- Aufbewahrungspflichten wurden nicht spezifiziert. Daten sind zu löschen, sofern die Aufbewahrung nicht mehr erforderlich ist.

Glossar

Begriff	Erläuterung
Anonymisierung / anonyme Daten	Die DS-GVO selbst definiert die Anonymisierung nicht. Nach EG 26 Satz 5 DS-GVO gilt die DS-GVO nicht für „anonyme Informationen […], d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Daten sind somit anonym i.d.S., wenn sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, wenn sie also nicht personenbezogen sind.
Auftragsverarbeiter	Ein Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Besondere Kategorien personenbezogener Daten	Besondere Kategorien personenbezogener Daten sind personenbezogene Daten i.S.v. Art. 9 Abs. 1 DS-GVO: Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
Betroffene Person	Eine betroffene Person ist gemäß Art. 4 Nr. 1 DS-GVO eine identifizierte oder identifizierbare natürliche Person, auf die sich verarbeitete Informationen beziehen.
Datenverarbeitungsanlagen	Datenverarbeitungsanlagen i.S.d. Kriterienkatalogs sind Geräte für die elektronische Verarbeitung von Daten (z. B. Server, Personal Computer oder Laptops einschließlich dazugehöriger Ein- und Ausgabegeräte), auf denen personenbezogene Daten im Zusammenhang mit dem schulischen Informationssystem des System-Anbieters verarbeitet werden.
Empfänger	Empfänger sind gemäß Art. 4 Nr. 9 DS-GVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden. Dies erfasst bspw. auch Auftragsverarbeiter, die eingesetzt werden, um bei der Erbringung des schulischen Informationssystems mitzuwirken.
Gemeinsam Verantwortliche / Gemeinsame Verantwortlichkeit	Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche i.S.v. Art. 26 i.V.m. Art. 4 Nr. 7 DS-GVO.
Informationssysteme / Schulische Informationssysteme	Informationssysteme sind soziotechnische Systeme, in denen digitale Technologien zur Verarbeitung von Informationen eingesetzt wird, z. B. zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung. Wenn Informationssysteme im Bereich der schulischen Bildung zum Einsatz kommen, werden sie als schulische Informationssysteme bezeichnet. S. hierzu ausführlich A. 2. a.
Metadaten	Metadaten sind Informationen, die andere Daten beschreiben. Sie liefern Kontext, Attribute und Details zu einem bestimmten Datensatz und helfen dabei, diesen zu organisieren, zu verstehen und zu verwalten. Einfacher ausgedrückt: Metadaten sind Daten über Daten.
Missbrauchsanfällige Funktionalitäten in Videokonferenzsystemen und anderen Kommunikationssystemen	Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann. Funktionalitäten, die genutzt werden können, um den Unterricht zu stören (z. B. durch das ständige Betreten

Begriff	Erläuterung
	und Verlassen oder das virtuelle Heben der Hand), sollten ebenfalls abschaltbar sein, werden von diesem Kriterium aber nur erfasst, wenn mit ihnen eine Verarbeitung personenbezogener Daten einhergeht.
Nachmittagsmarkt	Im Nachmittagsmarkt wird das schulische Informationssystem außerhalb des schulischen Bereichs als Lernmittel (z. B. zum selbstständigen Lernen oder zur Nachhilfe) herangezogen und hierfür insbesondere durch die Schülerinnen und Schülern bzw. von deren Erziehungsberechtigten angeschafft. Der System-Anbieter wird hier regelmäßig als Verantwortlicher auftreten.
Personenbezogene Daten	Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (= betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
Pseudonymisierung / pseudonyme Daten	Eine Pseudonymisierung ist gemäß Art. 4 Nr. 5 DS-GVO die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
Schulbehörde / Schulamt / Schulaufsicht	Die Schulbehörde ist eine staatliche Institution, die für die Verwaltung von Grundschulen, Hauptschulen und Förderschulen zuständig ist, wobei die obere Ebene vom Kultusministerium und die untere Ebene von den staatlichen Schulämtern auf der Kreis- bzw. Stadt-Ebene gebildet werden. Die übrigen Schulen wie berufliche Schulen werden direkt vom Kultusministerium beaufsichtigt.
Schulträger	Schulträger stellen als rechtsfähige Institutionen die sächlichen Bedingungen für eine Schuleinrichtung bereit und unterhalten diese. Das sind z. B. die räumlich-technischen Voraussetzungen sowie alle Ausstattung zur Sicherung von Unterricht und Erziehung einschließlich außerschulischer Kooperationen. In Deutschland sind öffentliche Schulträger meist Städte, Gemeinden und Landkreise, teilweise auch Bundesländer. Freie Träger können natürliche und juristische Personen sein, etwa Körperschaften des öffentlichen Rechts wie Landeskirchen, Diözesen oder Industrie-, Handels- und Handwerkskammer, aber auch eingetragene Vereine und Genossenschaften.
Stand der Technik	Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.
Subauftragsverarbeiter	Ein Subauftragsverarbeiter ist der Auftragsverarbeiter eines Auftragsverarbeiters (s. Art. 28 Abs. 2 und 4 DS-GVO, wobei der Begriff dort nicht verwendet wird).
System-Anbieter / System-Kunde / System-Nutzer	Zu den Begriffen s. A. 4. a.

Begriff	Erläuterung
TOM (technisch und organisatorische Maßnahmen)	TOM (technische und organisatorische Maßnahmen) ist ein Ober- und Sammelbegriff. TOM werden in der DS-GVO verschiedentlich erwähnt (vgl. z. B. Art. 5 Abs. 1 lit. f, Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 28 Abs. 1 und Art. 32 Abs. 1 DS-GVO). Es handelt sich um Maßnahmen, um den Datenschutz und die Datensicherheit zu gewährleisten. Während sich technische Maßnahmen auf den Verarbeitungsvorgang als solchen beziehen (z. B. Verschlüsselung oder Passwörter), betreffen organisatorische Maßnahmen (z. B. Führen eines Verzeichnisses von Verarbeitungstätigkeiten, Schulung von Mitarbeitenden). Insgesamt kann die Unterscheidung zwischen technischen und organisatorischen Maßnahmen aber nicht trennscharf vorgenommen werden.[68]
Übermittlung an Drittstaaten	Eine Übermittlung an Drittstaaten i.S.v. Art. 44 ff. DS-GVO liegt vor, wenn personenbezogene Daten aus der EU/dem EWR in ein Land oder mehrere Länder außerhalb der EU/des EWR übermittelt werden. Eine Übermittlung i.d.S. liegt auch vor, wenn die personenbezogenen Daten durch Fernzugriff einem Akteur außerhalb der EU/des EWR zugänglich gemacht oder mitgeteilt werden.
Verantwortlicher	Ein Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
Verarbeitung (personenbezogener Daten)	Verarbeitung bezeichnet gemäß Art. 4 Nr. 2 DS-GVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
Verarbeitungsvorgang	Kernelemente eines Verarbeitungsvorganges sind: 1. die personenbezogenen Daten (sachlicher Anwendungsbereich der DS-GVO), die verarbeitet werden, 2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und 3. Prozesse und Verfahren, die mit der Verarbeitung in Verbindung stehen. Ausführlich zu dem Begriff s. A. 2. b.
Verletzung des Schutzes personenbezogener Daten	Eine Verletzung des Schutzes personenbezogener Daten ist gemäß Art. 4 Nr. 12 DS-GVO eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
Vertreter (i.S.v. Art. 27 DS-GVO)	Ein Vertreter ist gemäß Art. 4 Nr. 17 DS-GVO eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Art. 27 DS-GVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt.
Vormittagsmarkt	Im Vormittagsmarkt wird das schulische Informationssystem direkt in den Unterricht an der Schule eingebunden. Der System-Anbieter wird regelmäßig als Auftragsverarbeiter des schulischen System-Kunden auftreten.

[68] Taeger/Gabel/*Lang*, Art. 24 DS-GVO Rn. 24.

Begriff	Erläuterung
Zugang	Zugang meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem).
Zugriff	Zugriff meint den Zugriff auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems.
Zutritt	Zutritt meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen.

Referenzen

Art.-29-Gruppe, WP 242 Rev.01	Art.-29-Gruppe, WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit, 5.4.2017, https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf.
Art.-29-Gruppe, WP 243 Rev.01	Art.-29-Gruppe, WP 243 Rev.01, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), 5.4.2017, https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf.
Art.-29-Gruppe, WP 248 Rev.01	Art.-29-Gruppe, WP 248 Rev. 01 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 4.10.2017, https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf.
Art.-29-Gruppe, WP 251 Rev.01	Art.-29-Gruppe, WP 251 Rev.01 Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 6.2.2018, https://ec.europa.eu/newsroom/article29/items/612053.
Art.-29-Gruppe, WP 260 Rev.01	Art.-29-Gruppe, WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679, 11.4.2018, https://ec.europa.eu/newsroom/article29/items/622227/en.
BayLDA, KI & Datenschutz	BayLDA, KI & Datenschutz, letzter Zugriff 17.02.2025, https://www.lda.bayern.de/de/ki.html
BeckOK Beamtenrecht Bund/*Bearbeiter*	BeckOK Beamtenrecht Bund, hrsg. v. Brinktrine/Schollendorf, 39. Edition, Stand 01.10.2025.
BeckOK Datenschutzrecht/*Bearbeiter*	BeckOK Datenschutzrecht, hrsg. v. Wolff/Brink/v. Ungern-Sternberg, 54. Edition, Stand 01.11.2025
BSI TR-02102 (alle Teile)	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 1-4. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, Stand 2025.
BSI, IT Grundschutz Kompendium	BSI, IT Grundschutz Kompendium, Stand Februar 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.
CNIL, AI how-to sheets	CNIL, AI how-to sheets, 7.6.2024, https://www.cnil.fr/fr/ai-how-to-sheets.
CNIL, AI system development	CNIL, AI system development, 7.6.2024, https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr.
DIN SPEC 27008	Basis IT-Sicherheitsmaßnahmen für Videokonferenz-Systeme. Stand 2024
DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme	DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme. Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 3.0 (17.11.2025), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/2025-DSK-Zertifizierungskriterien-Version_3.0.pdf.
DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO	DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, Februar 2018, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf.
DSK, Kurzpapier Nr. 1	DSK, Kurzpapier Nr. 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf.
DSK, Kurzpapier Nr. 4	DSK, Kurzpapier Nr. 4: Datenübermittlung in Drittländer, 22.7.2019, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.
DSK, Kurzpapier Nr. 5	DSK, Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.
DSK, Kurzpapier Nr. 6	DSK, Kurzpapier Nr. 6: Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf.
DSK, Kurzpapier Nr. 10	DSK, Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung, 16.1.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf.

DSK, Kurzpapier Nr. 13	DSK, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.
DSK, Kurzpapier Nr. 17	DSK, Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten, 27.3.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf.
DSK, Kurzpapier Nr. 18	DSK Kurzpapier 18: Risiko für die Rechte und Freiheiten natürlicher Personen, 26.4.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.
DSK, Kurzpapier Nr. 19	DSK, Kurzpapier Nr. 19: Unterrichtung und Verpflichtung von Beschäftigten Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO, 29.5.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf.
DSK, Orientierungshilfe Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung	DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung, 29.03.2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_anbieter_onlinedienste.pdf.
DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)	DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste), November 2024, https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf.
DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht	DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 26.4.2018, https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf.
DSK, Orientierungshilfe Künstliche Intelligenz und Datenschutz	DSK, Orientierungshilfe: Künstliche Intelligenz und Datenschutz, 6.5.2024, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.
DSK, Orientierungshilfe Mandantenfähigkeit	DSK, Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur. Orientierungshilfe Mandantenfähigkeit, 11.10.2012, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenf%C3%A4higkeit.pdf.
DSK, Orientierungshilfe zu Videokonferenzsystemen	DSK, Orientierungshilfe Videokonferenzsysteme, 23.10.2020, https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf.
EDSA, Empfehlungen 01/2020	EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten, 18.6.2021, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf.
EDSA, Empfehlungen 02/2020	EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10.11.2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf.
EDSA, Empfehlungen 1/2022	EDSA, Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO), 30.06.2023, https://www.edpb.europa.eu/system/files/2024-05/edpb_recommendations_20221_bcr-c_v2_de.pdf.
EDSA, Guidelines 01/2025	EDSA, Guidelines 01/2025 on Pseudonymisation, 16.1.2025, https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.
EDSA, Leitlinien 4/2019	EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, 20.10.2020, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf.
EDSA, Leitlinien 07/2020	EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und

	„Auftragsverarbeiter" in der DSGVO, 7.7.2021, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf.
EDSA, Leitlinien 4/2021	EDSA, Leitlinien 04/2021 über Verhaltensregeln als Instrument für Übermittlungen, 22.2.2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de.
EDSA, Leitlinien 5/2021	EDSA, Leitlinien 5/2021 zum Zusammenspiel zwischen Art. 3 und Kapitel V der Datenschutz-Grundverordnung, 14.2.2023, Version 2.0, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.
EDSA, Leitlinien 9/2022	EDSA, Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO, 28.3.2023, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_de_0.pdf.
EDSA, Stellungnahme 22/2024	EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben, 7.10.2024, https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202422_relianceonprocessors-sub-processors_de_0.pdf.
EGMR, Factsheet – mass surveillance	EGMR, Factsheet – mass surveillance, June 2024, https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.
Ehmann/Selmayr/*Bearbeiter*	Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024
EU-SVK	Europäische Kommission, Durchführungsbeschluss vom 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der DS-GVO, https://ec.europa.eu/info/sites/default/files/1_de_act_part1_v3_1.pdf.
HmbBfDI, Checkliste zum Einsatz LLM-basierter Chatbots	HmbBfDI Checkliste zum Einsatz LLM-basierter Chatbots, 13.11.2023, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checkliste_LLM_Chatbots_DE.pdf.
ISO/IEC 11770 (alle Teile)	Informationstechnik - Sicherheitsverfahren - Schlüsselmanagement - Teil 1-7
ISO/IEC 20889	Informationstechnik – Sicherheitsverfahren - Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre. Stand 2018
ISO/IEC 21964 (alle Teile)	Informationstechnik - Bürogeräte - Vernichten von Datenträgern - Teil 1-3
ISO/IEC 2382	Informationstechnik – Vokabular. Stand 2015
ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen. Stand 2022
ISO/IEC 27040	Informationstechnik - IT-Sicherheitsverfahren - Speichersicherheit. Stand 2015
ISO/IEC 27701	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Datenschutz-Informationsmanagementsysteme - Anforderungen und Leitlinien. Stand 2025
ISO/IEC 27555	Informationssicherheit, Cybersicherheit und Datenschutz - Leitlinien zur Löschung personenbezogener Daten. Stand 2021
ISO/IEC 29101	Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur. Stand 2018
ISO/IEC 29134	Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung. Stand 2017
ISO/IEC 29146	Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung. Stand 2016
ISO/IEC 30111	Informationstechnik – IT-Sicherheitsverfahren - Prozesse für die Behandlung von Schwachstellen. Stand 2019.
ISO 31000	Risikomanagement - Leitlinien. Stand 2018
IEC 31010	Risk management - Risk assessment techniques. Stand 2019
Länderberichte	Inter-American Commission on Human Rights, Country Reports, https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/reports/country.asp.

LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz	LfDI BW Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0, 17.10.2024, https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki.
Paal/Pauly/*Bearbeiter*	Paal/Pauly, Datenschutzgrundverordnung Bundesdatenschutzgesetz, 4. Auflage, München 2026.
SDM	Standard-Datenschutzmodell, Version 3.1, 14.5.2024, https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf.
SDM-Baustein 11	SDM-Baustein 11 „Aufbewahren“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Aufbewahren_V1.0.pdf.
SDM-Baustein 41	SDM-Baustein 41 „Planen und Spezifizieren“, Version 1.0, 25.3.2021, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Planen_Spezifizieren_V1.0.pdf.
SDM-Baustein 42	SDM-Baustein 42 „Dokumentieren“, Version 1.0a, 2.9.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Dokumentieren_V1.0a.pdf.
SDM-Baustein 50	SDM-Baustein 50 „Trennen“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf.
SDM-Baustein 51	SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, Version 1.0, 1.11.2021, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Zugriffe_regeln_V1.0.pdf.
SDM-Baustein 60	SDM-Baustein 60 „Löschen und Vernichten“, Version 1.0a, 2.9.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf.
SDM-Baustein 61	SDM-Baustein 61 „Berichtigen“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Berichtigen_V1.0.pdf.
SDM-Baustein 62	SDM-Baustein 62 „Einschränken der Verarbeitung“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Einschr%C3%A4nken_V1.0.pdf.
Simitis/*Bearbeiter*	Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014.
Simitis/Hornung/Spiecker gen. Döhmann/*Bearbeiter*	Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht DSGVO/BDSG, 2. Auflage 2025.
Taeger/Gabel/*Bearbeiter*	Taeger/Gabel, DSGVO – BDSG – TDDDG, 4. Auflage 2022.
Teletrust, Handreichung zum Stand der Technik	Teletrust, Handreichung zum „Stand der Technik“. Technische und organisatorische Maßnahmen, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf, Stand: 2021.

directions